Каторин Ю. Ф., Куренков Е. В., Лысов А. В.,
Остапенко А. Н.

# Большая энциклопедия промышленного шпионажа

ПОЛИГОН
Санкт-Петербург
2000

## АННОТАЦИЯ

Каторин Ю. Ф., Куренков Е. В., Лысов А. В., Остапенко А. Н.
**Большая энциклопедия промышленного шпионажа**
ПОЛИГОН
Санкт-Петербург
2000
ББК 67.99(2)116.2
К 29
Под общей редакцией Е. В. Куренкова
**Каторин Ю. Ф., Куренков Е. В., Лысов А. В., Остапенко А. Н.**
К 29 Большая энциклопедия промышленного шпионажа. — СПб.: 000 «Издательство Полигон», 2000. — 896 с., ил.
ISBN 5-89173-106-1
Эта книга наиболее полно освещает вес основные современные способы негласного съема информации и методы защиты от промышленного шпионажа. Энциклопедический характер изложенного материала, рассмотрение широкого круга аспектов информационной безопасности делают настоящее издание настольной книгой для представителей государственных органов и сотрудников служб безопасности, преподавателей, студентов и других лиц, обеспокоенных проблемой защиты информации. Книга может использоваться как учебное пособие и как справочник для специалистов, имеющих опыт практической работы. Надеемся, что она будет интересна и для людей, впервые столкнувшихся с этой проблемой.
ББК 67.99(2)116.2

1992. — 206р.
Научно-популярное издание
**Каторин Юрий Федорович**
**Куренков Евгений Владимирович**
**Лысов Андрей Владимирович**
**Остапенко Александр Николаевич**
**БОЛЬШАЯ ЭНЦИКЛОПЕДИЯ ПРОМЫШЛЕННОГО ШПИОНАЖА**
Главный редактор Н. Л. Волковский
Редактор И. В. Петрова
Корректор А. Ю. Ларионова
Компьютерная графика О. И. Орлова
Компьютерная верстка С. А. Елисеева
Зав. производством Е. С. Фоменко
Подписано в печать с готовых диапозитивов 04.08.2000. Формат 70xl001/16. Гарнитура TimeRoman. Печать офсетная. Физ. печ. л. 56,0. Усл. печ. л. 72,24. Тираж 10 000 экз. Заказ № 105.
Налоговая льгота — общероссийский классификатор продукции ОК-00-93, том 2; 953 000 — книги, брошюры
000 «Издательство «Полигон», 191126, С.-Петербург, а/я 80. Тел.: 329-74-24; тел./факс: 320-74-23 Для писем: 191119, С.-Петербург, а/я 80
E-mail: polygon@spb.cityline.ru
ОАО «Санкт-Петербургская типография № 6». 193144, Санкт-Петербург, ул. Моисеенко, д. 10. Телефон отдела маркетинга 271-35-42.

**ОГЛАВЛЕНИЕ**

(1994 г.).
«О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны». Постановление Правительства РФ.
«О сертификации средств защиты информации». Постановление Правительства РФ.
ГОСТ Р 51275-99. Защита информации. Объект информации. Факторы, воздействующие на информацию
«Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации
от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники». Руководящий документ Гостехкомиссии РФ.
«Положение о Государственном лицензировании деятельности в области защиты информации». Совместное решение Гостехкомиссии России и ФАПСИ.
«Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации». Руководящий документ Гостехкомиссии РФ.
«Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». Руководящий документ Гостехкомиссии РФ
«Средства вычислительной техники. Защита от НСД к информации.
Показатели защищенности от НСД к информации». Руководящий документ Гостехкомиссии РФ.
«Средства вычислительной техники. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации». Руководящий документ Гостехкомиссии РФ.
«Защита от несанкционированного доступа к информации». Руководящий документ Гостехкомиссии РФ.
«Защита информации. Специальные защитные знаки. Классификация и общие требования». Руководящий документ Гостехкомиссии РФ.
2.2. Организация защиты информации
2.2.1. Основные понятия информационной безопасности
2.2.2. Организационные мероприятия по защите информации
2.2.3. Добровольная аттестация объектов информатизации по требованиям безопасности информации
2.3. Методы и средства выявления закладных устройств
2.3.1. Общие принципы выявления
2.3.2. Индикаторы поля
2.3.3. Специальные радиоприемные устройства
2.3.4. Программно-аппаратные комплексы
2.3.5. Нелинейные радиолокаторы
2.3.6. Некоторые рекомендации по поиску устройств негласного «съема информации
2.4. Технические средства защиты информации в помещениях и сетях связи
2.4.1. Общие принципы защиты
2.4.2. Аппаратура контроля линий связи
2.4.3. Средства защиты линий связи
2.4.4. Криптографические методы и средства защиты
2.4.5. Защита от пиратских подключений
2.4.6. Технические средства пространственного и линейного зашумления
2.4.7. Защита информации от высокочастотного навязывания
2.5. Защита от несанкционированной аудиозаписи
2.5.1. Обнаружители диктофонов
2.5.2. Устройства подавления записи работающих диктофонов
2.6. Защита информации в компьютерных сетях
2.6.1. Виды потенциально опасных воздействий
2.6.2. Защита от ошибок обслуживающего персонала
2.6.3. Защита от заражения компьютерными вирусами
2.6.4. Программно-аппаратные средства защиты информации от несанкционированного доступа

## ВВЕДЕНИЕ

Данная книга не является продолжением или дополнением к недавно выпущенной «Энциклопедии промышленного шпионажа», хотя и написана на ее основе, а представляет собой новую и практически самостоятельную работу, в которой ликвидированы основные недостатки старой. От предыдущей книги она отличается не только существенно большим объемом, но и совершенно другой концепцией подачи материала. Авторы не просто описывают те или иные устройства, а подробно рассказывают об их принципе действия, достоинствах и недостатках, дают подробные советы по практическому применению.
На современном этапе, когда произошла коренная переоценка ценностей, многие традиционные ресурсы человеческого прогресса утрачивают свое первостепенное значение. Но информация как была, так и остается одним из главных ресурсов научно-технического и социально-экономического развития мирового сообщества. Мало того, очень скоро хорошо налаженная информационная сеть будет призвана сыграть в повседневной жизни такую роль, какую в свое время сыграли электрификация, телефонизация, радио и телевидение вместе взятые. Информация влияет не только на ускорение прогресса в науке и технике, но и на обеспечение охраны общественного порядка, сохранности собственности, общение между людьми и другие социально значимые области. Воистину она пронизывает все сферы жизнедеятельности людей, ибо в основе любого решения — информация. И чем объем и достоверность имеющейся у вас информации выше, тем, как правило, выше и оптимальность принятого решения. И наоборот, чем меньшим объемом информации о вас владеет ваш конкурент, тем шире у вас простор для маневра.
Поэтому информация может быть использована особой категорией населения в преступных и других антигуманных целях. Она также может стать в руках ненадежных и эксцентричных людей грозным оружием в борьбе с конкурентом или при ведении «войны компроматов». Примеры таких деяний так часто мелькают в газетах и на экранах, что на них уже почти перестали обращать внимание, если это не что-то из ряда вон выходящее, например, обнаружение подслушивающего устройства в кабинете главного редактора «Комсомольской правды» (1998) или скандал с фирмой «Атолл» (февраль 1999 года), которая будто бы прослушивала разговоры даже членов семьи президента; или ликвидация правоохранительными органами стационарного пункта для осуществления прослушивания сотовых и спутниковых телефонов, а так же переговоров своих сотрудников в холдинге «Медиа-МОСТ» (май 2000 года). Поэтому очень актуальной становится проблема обеспечения информационной безопасной деятельности не только

государственного служащего (что у нас всегда было на высоте), но и бизнесмена, предпринимателя, юриста, публичного политика, да и просто достаточно известного в обществе человека.

По мнению компетентных экспертов, в случае полного рассекречивания информации о деятельности коммерческой фирмы последняя в условиях нашего «дикого» рынка просуществует от нескольких часов до нескольких дней. Аналогичная участь ожидает и подавляющее большинство коммерческих банков. Не менее серьезными могут быть последствия в случае утечки каких-нибудь материалов, компрометирующих политика или крупного бизнесмена. Такой человек легко может стать объектом шантажа и даже полностью утратить самостоятельность действий. Здесь вспоминается громкое дело «голого министра», стоившее в 1998 году карьеры министру юстиции России В. Ковалеву и в конечном итоге доведшее его до «Бутырки». И другой пример, когда в аналогичной ситуации оказался Генеральный прокурор Ю. Скуратов.

Главное завоевание перестройки — свободная пресса,— как оказалось, имеет и другую сторону медали: некоторые издания начали подлинную охоту за знаменитостями. Притом охоту весьма специфическую: любым способом добываются «жареные факты», интимные подробности, семейные скандалы и весь этот мутный поток выплескивается на читателя. Жертвами таких доморощенных папарацци уже стали некоторые наши эстрадные звезды и даже крупные бизнесмены.

Таким образом, проблема защиты информации и обеспечения конфиденциальности личной жизни приобретает актуальность для очень многих людей, чья деятельность находится вне области, где эти вопросы решают государственные органы. И, конечно, каждому хочется для укрепления своей безопасности использовать самые надежные современные методы и средства, учитывающие все особенности приемов несанкционированного добывания сведений. Раз есть спрос, то будет и предложение. Но, к большому сожалению, к этой деятельности, как и к любому делу, сулящему деньги, обратилось довольно много некомпетентных, а иногда попросту нечестных людей.

Положение усугубляется еще и тем, что из-за своеобразного хода истории современный российский предприниматель не имеет традиций поведения в условиях промышленного шпионажа. Так, если в дореволюционной России, где существовал весьма развитый рынок услуг по получению любых сведений о конкурентах или потенциальных партнерах, любой предприниматель был всегда настороже и четко знал основные правила поведения, а также приемы и способы защиты, то в Советской России коммерческая тайна была отменена официально «Положением о рабочем контроле», принятом ВЦИК в ноябре 1917 года. Вместо рынка ввели распределительную систему, конкуренцию заменили соцсоревнованием, а все предприятия обязали непременно обмениваться опытом. Однако справедливости ради надо отметить, что военную и государственную тайну хранить умели, и притом с эффективностью, которой на Западе могли только позавидовать (об этом свидетельствуют весьма поучительные мемуары наших «бывших» противников).

Развитие рыночных отношений, развал очень жесткой системы контроля за ввозом и производством специальной техники, массовый уход из бывшего КГБ, ГРУ и МВД профессионалов высшего класса — все это привело к возрождению буквально за два-три года рынка услуг по добыванию информации о конкурентах. Но рынка с «русской спецификой»: к относительно немногочисленным «профи», действующим осторожно и эффективно (поэтому и борьба с ними — дело тоже сугубо для профессионалов), прибавились многочисленные шпионы-любители, когда-то нахватавшиеся поверхностных знаний на каких-нибудь краткосрочных курсах или просто начитавшиеся детективов.

Но и эти дилетанты находят своих клиентов, потому что, как правило, на уровне читателя такого рода романов находятся знания и у объектов их внимания. Именно это и открывает широкое поле деятельности для разного рода мошенников и проходимцев. Некоторые из них, всевозможными путями приобретя самую примитивную аппаратуру, открывают сомнительные частные сыскные агентства по добыванию информации любого рода и даже, бывает, добиваются определенных результатов, конечно, если не встречают хоть самого простого противодействия. Другие, наоборот, открывают различные конторы с громкими названиями по защите информации, а в ряде случаев одна и та же фирма ведет оба вида деятельности. Польза от таких «защитников» при серьезной угрозе практически нулевая, а правильней сказать — со знаком минус, поскольку они дают людям ложную иллюзию защищенности, что невольно расслабляет человека. И хотя беспредел начала 90-х годов в этой сфере деятельности, наконец,

подходит к концу, прохиндеи дело не сворачивают, а лишь уходят «в тень».
Чтобы не стать жертвой ни одной из разновидностей этих мошенников, лицам, имеющим дело с конфиденциальной информацией, просто жизненно необходимо обладать некоторой подготовкой и достаточно квалифицированно ориентироваться во всем спектре вопросов обеспечения информационной безопасности, понимать их комплексный и взаимообусловленный характер.
Несмотря на появившиеся в большом количестве книги, посвященные защите информации, далеко не все из них отвечают интересам читателей. Зачастую это подробное рассмотрение некоторых частных аспектов, понятных лишь специалисту, либо, наоборот, чересчур поверхностное рассмотрение достаточно важных практических вопросов. Последние, конечно, читаются с интересом, но никакой практической пользы принести не могут. Этот пробел и решили заполнить выпуском данной книги сотрудники Санкт-Петербургской Лаборатории противодействия промышленному шпионажу (Лаборатория ППШ), Федерального государственного унитарного предприятия «Научно-производственное предприятие "Гамма"» (ФГУП НПП «Гамма») и кафедры радиоэлектронной борьбы и защиты информации Военного инженерно-космического университета имени А. Ф. Можайского, которые многие годы профессионально занимаются проблемами защиты информации.
Идея книги возникла в 1992 году после двух первых «контактов» с мошенниками. Тогда в Лабораторию ППШ, которая только обрела свой статус, обратился один из городских коммерческих банков с просьбой дать консультацию по поводу предложений некоего совершенно непонятного совместного предприятия (СП) о разработке концепции информационной безопасности для этого финансового учреждения. Двое иностранных граждан, заручившись самыми высокими рекомендациями (правда, не специалистов, а чиновников совсем другого профиля), настойчиво осаждали руководство банка и заявляли, что готовы за три дня «на основе самых последних достижений американской науки» создать для них «самую точную концепцию защиты всей информации банка». При этом они рассказывали множество «ужасающих» историй о крахах и ограблениях тех банков, которые не захотели воспользоваться их помощью. Мы попросили разрешения присутствовать на встрече с новоявленными «информационными гениями».
В кабинет управляющего вошли два очень энергичных молодых человека, и на присутствующих полился поток слов и терминов, многие из которых, кстати, никакого отношения к делу не имели. На вопрос: «Сколько стоит разработка концепции?»— последовал мгновенный ответ: «17 650 долларов!» Вопрос о том, сколько будет стоить обеспечение безопасности одного рабочего места, на секунду вызвал замешательство, но потом опять полились слова о том, что концепция — это не мелкие детали, а стратегия. **Зато** вопросы о перекрываемых каналах утечки, сертификации и примерном перечне аппаратуры привели к тому, что наши бывшие земляки, а ныне американские «гринкартовцы» весьма поспешно ретировались. Случай, конечно, уникальный по своей наглости, но он заставил нас задуматься о том, что даже очень грамотные в своей области люди (руководители банка), могут быть полными профанами в другой, и прав был незабвенный Козьма Прутков: «Специалист подобен флюсу: полнота его односторонняя».
Через некоторое время в Лабораторию ППШ за помощью обратился генеральный директор небольшого ликеро-водочного завода. Бизнесмен заподозрил, что у него идет утечка информации, поскольку один из его клиентов всегда четко торгуется до предельной цены, только-только согласованной на закрытом совещании. Предположение о применении подслушивающих устройств было с негодованием отвергнуто начальником службы безопасности, а директор с неподдельной гордостью заявил, что он человек прогрессивный и не просто проверяет свой офис раз в месяц, но и имеет договор с некой фирмой. «Только три дня назад все здесь обследовали, — сказал он. — Бегали по всему заводу с приемниками». Последняя фраза нас насторожила, и мы все-таки уговорили винокуров провести проверку. Через полчаса перед потрясенным директором (надо отдать должное его чутью коммерсанта, он правильно заподозрил в нечестности своего партнера) были выложены два примитивных самодельных подслушивающих устройства, которые профессионал просто не мог не обнаружить. Более подробные расспросы позволили сделать вывод, что «проверка» фирмы сводилась к тому, что 5—б человек, вооружившись спортивными приемниками для «охоты на лис», изображали попытки что-то запеленговать. Из всех приемников «лисолов», пожалуй, наименее пригоден для обнаружения «жучков» в помещении, но зато имеет очень внушительный

внешний вид, что и стало решающим аргументом для самозванцев. По просьбе директора его начальник службы безопасности (бывший спецназовец) посетил несколько занятий в Лаборатории ППШ, и мы уверены, что таких проколов у него больше не будет.

Кроме этих, по-своему даже и курьезных, случаев сотрудникам Лаборатории пришлось столкнуться и с подлинными человеческими трагедиями, когда в одночасье терялись нажитые тяжелым трудом капиталы, терпели крах фирмы, разорялись акционеры, и все из-за пренебрежения элементарными правилами безопасности. Это еще больше убедило нас в необходимости появления книги, где в форме, доступной для любого грамотного человека, но не имеющего специального образования, были бы изложены основные правила обеспечения безопасности информации, притом охватывающей все стадии этого процесса: от оценки угрозы до реализации собственной системы защиты.

Однако в начале 90-х годов все наши обращения в солидные издательства заканчивались тем, что, ознакомившись с планом книги, редактор категорически отказывался от этой тематики (глубоко в нас еще сидит тоталитарное «низя»). В 1994 году тиражом в 1000 экземпляров силами Лаборатории все-таки была выпущена брошюра «Промышленный шпионаж в России: методы и средства». Ее успех укрепил нашу решимость добиться издания полноценной книги, и мы очень благодарны издательству «Полигон», которое сразу согласилось оказать нам содействие.

В ноябре 1999 года эта работа, получившая название «Энциклопедия промышленного шпионажа», вышла в свет. И хотя тираж был относительно небольшой, но, судя по довольно многочисленным отзывам, книга дошла до широкого читателя. Мы очень благодарны всем, кто в какой-либо форме нашел время высказать свои замечания по нашей работе. Отзывы можно разделить на две группы.

В первую группу следует включить мнения, высказанные людьми, которые профессионально занимаются вопросами защиты информации. Особенно нас порадовало то, что в целом их мнение о работе вполне доброжелательное. Вместе с тем, есть и целый ряд критических замечаний. Если их обобщить, то они сводятся к следующему.

Во-первых, приведенные нами цены на продукцию тех или иных фирм не соответствуют текущей цене на момент выхода книги. Конечно, сам процесс выпуска книги — довольно долгая процедура, а цены на рынке меняются почти каждый день. Поэтому, несмотря на все просьбы потенциальных покупателей, мы убедились, что, к сожалению, следует убрать из работы упоминание о точной стоимости конкретных приборов.

Во-вторых, ряд организаций обиделись на нас за то, что мы описали аппаратуру, выпускаемую конкурентами, но умолчали об их продукции. Сразу же хотим подчеркнуть, что при рассказе о конкретных моделях мы описывали характерных представителей того или иного класса спецтехники, исходя только из необходимости проиллюстрировать ее практические возможностей, а совсем не ставили задачу проанализировать все существующие модели и выбрать лучшие. Такая книга могла бы быть интересна для узкого круга специалистов, но вряд ли устроила бы широкого читателя. Вместе с тем, название нашей работы обязывает к более подробному освещению рынка спецтехники (далеко не все покупатели могут «нырнуть» в соответствующие сайты Интернета), поэтому мы приняли решение существенно увеличить объем материала, который посвящен описанию серийных приборов.

В-третьих, несколько уважаемых организаций сделали нам замечание, что мы описали модели их приборов, уже снятые с производства. Данную претензию трудно назвать обоснованной, поскольку у любой продукции есть и так называемый вторичный рынок.

В-четвертых, поступили просьбы увеличить количество приведенных принципиальных схем устройств как для защиты, так и для съема информации, поскольку это позволит серьезным частным охранным структурам более эффективно организовать работу службы технической безопасности. С удовольствием выполняем это пожелание в части, касающейся устройств защиты.

Ко второй группе отзывов следует отнести пожелания, высказанные непрофессионалами. Именно эти отзывы и представили для авторов наибольшую ценность, поскольку книга была рассчитана в первую очередь на широкого читателя или начинающих сотрудников службы безопасности. В целом пожелания этой категории можно свести к следующему.

Во-первых, практически все позвонившие или сбросившие факсы просили дать конкретные рекомендации по применению того или иного класса аппаратуры для защиты своих офисов или квартир. Сразу хотим сказать, что 100-процентный успех будет только в том случае, если специалист подробно ознакомится с деталями и задачами операции по

перекрытию того или иного канала утечки. Консультацию, притом бесплатную, по выбору конкретного прибора можно легко получить по телефону или в личной беседе, посетив Лабораторию ППШ. Мы решили в данной книге более подробно рассказать обо всех особенностях применения основных средств противодействия промышленному шпионажу. Указать их сильные и слабые (да простят нас разработчики, но мы вынуждены это сделать) стороны. Ознакомление с этим материалом поможет читателям не попадать в положение некоторых поздно обратившихся к нам клиентов, единственной рекомендацией для которых по применению самостоятельно купленной спецтехники было: «Постарайтесь побыстрее ее продать».

Во-вторых, почти все, связавшиеся с нами, просили привести возможно большее количество принципиальных схем именно тех простейших приборов защиты, которые можно бы было сделать в домашних условиях. Конечно, цены на фирменную спецтехнику очень высокие, но нужно четко понимать, что самоделка, как правило, может защитить тоже только от самоделки. Однако, учитывая наличие весьма насыщенного «черного» рынка шпионской техники, выполняем и это пожелание. В новой книге приведены принципиальные схемы и дано подробное описание тех типов аппаратуры защиты, которые сможет сделать самостоятельно даже радиолюбитель средней руки.

В-третьих, поступили просьбы более подробно рассказать о принципе действия тех или иных устройств защиты. В том объеме, который не затрагивает секретов ноу-хау, реализуем и это предложение. Нам вполне понятно желание клиентов, говоря словами А. В. Суворова, «знать свой маневр».

В-четвертых, поступили многочисленные просьбы указать перечень организаций, которые имеют право заниматься вопросами, связанными с защитой информации. По мере возможностей выполняем и это пожелание. Естественно, что полный перечень привести может только Гостехкомиссия при Президенте РФ, но самые авторитетные фирмы мы укажем в приложении. В книге приведен образец гослицензии, наличие которой только и дает право на занятие такого рода деятельностью. Поэтому если такой документ у вашей местной организации есть, то уже одно это является вполне надежной гарантией ее достаточно высокой профессиональной квалификации.

И наконец, все читатели, приславшие свои отзывы и пожелания, задали один и тот же вопрос: «Насколько велика вероятность столкнуться с промышленными шпионами на практике?» В связи с этим мы решили рассказать о некоторых случаях применения спецтехники, о которых стало известно широкому кругу лиц, поскольку из профессионально-этических соображений у нас, увы, нет возможности сослаться на свой богатый личный опыт.

Анализ намеченных нами изменений и дополнений привел к тому, что стало ясно — просто вторым изданием, пусть оно даже будет исправленным и дополненным, в данном случае не обойтись. Поэтому было принято решение выпустить новую книгу. Данное издание хотя и содержит в себе практически всю ту полезную информацию, что была и в предыдущем, но по сути представляет собой совершенно другую работу. Первая книга в значительной степени носила сугубо описательный характер: мы давали читателю сведения о тех или иных приборах, а выводы предоставляли делать самому. Новая книга, сохранив описания технических характеристик, дополнительно содержит сведения об особенностях применения различных видов спецтехники, о принципе ее действия, основных преимуществах и недостатках. Таким образом, не просто вырос объем материала, а изменилась сама концепция нашей работы.

Новая книга также состоит из двух частей. В первой части изложены основные методы, которыми пользуются для несанкционированного доступа к информации, при этом акцент сделан на технические средства. Описаны практически все виды подслушивающей (в широком смысле этого слова) аппаратуры, которые используются в промышленном шпионаже, приемы и тактика ее применения. Для специалистов приведены и схемы некоторых устройств, чтобы было более понятно, как они работают, а значит, почему защита от них осуществляется тем или иным способом. Номиналы элементов на схемах не приводятся либо изменены, так как у нас нет желания делать руководство для доморощенных шпионов. Любителям в очередной раз хочется напомнить, что эта работа требует не только специального образования, но и значительных денег, и самое главное — большого ума. Конечно, книга не может охватить все без исключения методы и средства, о некоторых авторы умышленно умалчивают, поскольку не пришло еще время, и не хотелось бы создавать трудности правоохранительным органам в работе по защите

нас с вами от преступников и иностранных шпионов. Цель этой части — дать реальное представление о возможностях злоумышленников и заодно развеять некоторые устоявшиеся литературные мифы (увы, далеко не все авторы детективов владеют этим сложным материалом). Будем считать, что это — одна сторона медали.

Вторая часть посвящена вопросам организации защиты информации от несанкционированного доступа. Обеспечить 100-процентную защиту на все случаи жизни, конечно, невозможно, поэтому основным критерием ее эффективности служит соотношение финансовых затрат нарушителя на преодоление системы защиты и стоимости полученной информации. Если последняя — меньше затрат нарушителя, то уровень защиты считается достаточным. Поэтому в книге не описаны очень дорогие, экзотические методы и приведены средние цены как на аппаратуру съема информации, так и на аппаратуру ее защиты. Достаточно подробно рассмотрены и нормативно-правовые аспекты, регламентирующие информационные отношения в обществе.

Для тех, кто не ожидает угрозы своей деятельности от серьезных структур и собирается самостоятельно осуществлять защиту только от шпионов-любителей, достаточно подробно освещены организационные и технические мероприятия, позволяющие справиться с этой задачей. Приведен перечень, а также описаны принцип действия, технические характеристики и приемы работы с основными видами аппаратуры контроля и поиска устройств, предназначенных для скрытого съема информации. Схемы этой части уже имеют все необходимые номинации для их изготовления. Конечно, в таких деталях приведены только самые простейшие приборы, чтобы их можно было изготовить в домашних условиях. Данный материал будет полезен и тем гражданам, которые уже прибегают к услугам профессионалов. Во-первых, чтобы понимать их действия, а во-вторых, чтобы не стать жертвой мошенников, как питерские виноделы. Это вторая, и самая важная, сторона.

Вместе с тем, авторы не пытались изложить материал как полные знания, необходимые специалисту, что и невозможно в одной книге, а главным образом стремились через этот материал дать представление об основных методах и направлениях защиты информации, которые реально используются или могут быть использованы в ближайшее время. Надеемся, что бизнесмены, юристы, руководители частных служб безопасности, да и просто люди, по разным причинам ставшие носителями коммерческих или других секретов, прочитав книгу, получат представление о реальных возможностях злоумышленников и мерах противодействия им.

В настоящем издании наряду с нашим личным опытом использованы и другие материалы из области защиты информации, которые были опубликованы и показались нам интересными. Мы выражаем благодарность всем авторам, чей труд помог в работе над этим изданием. Полный перечень использованной литературы приведен в конце книги.

Особую признательность авторы выражают всем сотрудникам кафедры радиоэлектронной борьбы и защиты информации Военного инженерно-космического университета имени А. Ф. Можайского, Лаборатории ППШ, ФГУП НПП «Гамма», а также кафедры оперативно-технического обеспечения деятельности ОВД Санкт-Петербургского университета МВД России, оказавшим существенную помощь в работе над рукописью.

Авторы будут рады выслушать мнение об изложенном материале, как от специалистов, так и от любых заинтересованных лиц. Ваши отзывы и пожелания просим направлять по адресам:

**190000, Россия, Санкт-Петербург, переулок Гривцова, 1/64, Лаборатория ППШ, тел.: (812) 219-11-37,314-22-59 факс: (812) 315-83-75 E-mail: postmaster@pps.spb.su Website: http://www.pps.ru**

**197110, Россия, Санкт-Петербург, ул. Пионерская, 44, ФГУП НПП «Гамма», Представительство по Северо-Западному региону, тел/факс 235-55-18, E-mail: gamma@peterlink.ru**

# Глава первая

## ПРОМЫШЛЕННЫЙ ШПИОНАЖ

### 1.1. Промышленный шпионаж и закон

Понятие промышленный шпионаж не ново, оно возникло вместе с появлением

промышленности и является неотъемлемой частью отношений в странах, где наряду с государственной существуют и другие формы собственности.
Сущность промышленного шпионажа — это стремление к овладению секретами конкурентов с целью получения максимальной коммерческой выгоды. Он заключается в получении любой информации о новейших научно-технических разработках (ноу-хау(См.Сноску 1)), коммерческих планах, состоянии дел и т. п. Ведется всеми доступными средствами, включая применение специальных технических средств и подкуп должностных лиц.
Однако несмотря на то, что промышленный шпионаж в прямой постановке не затрагивает интересы государства, он является незаконным видом деятельности, так как покушается на конституционные права граждан. Государство стоит на защите этих прав, а значит их нарушение ведет к уголовной ответственности.
В связи с вышесказанным авторы не ставили себе задачу выпустить практическое руководство по ведению промышленного шпионажа. Наоборот, **защита от недобросовестных конкурентов — вот истинная цель настоящей книги.** В то же время нельзя победить «противника», ничего не зная о нем, поэтому первая часть посвящена именно применению методов и средств негласного получения конфиденциальной информации.
Права граждан на защиту их личной и коммерческой тайны подробно будут рассмотрены в разделе 2.1. Здесь же отметим, что в соответствии со **статьей 13** закона **«Об оперативно-розыскной деятельности»** (в редакции от 5 июля 1995 года), право на негласное получение информации с использованием специальных технических средств имеют только те органы, которым разрешено осуществлять оперативно-розыскную деятельность на территории Российской Федерации. К ним относятся:

___
Сноска 1. Ноу-хау (от англ. know how) — дословно «знаю как».

___
>- органы внутренних дел Российской Федерации;
>- органы федеральной службы безопасности;
>- федеральные органы налоговой полиции;
>- федеральные органы государственной охраны: Главное управление охраны Российской Федерации и Служба безопасности Президента Российской Федерации;
>- органы пограничной службы Российской Федерации;
>- таможенные органы Российской Федерации;
>- Служба внешней разведки Российской Федерации;
>- органы внешней разведки Министерства обороны Российской Федерации;
>- органы внешней разведки Федерального агентства правительственной связи и информации при Президенте Российской Федерации.
Однако сотрудники этих подразделений не могут по первому желанию вторгаться в личную жизнь граждан, так как **статья 8** упомянутого закона определяет условия проведения соответствующих оперативно-розыскных мероприятий. В частности, в ней сказано:
...Проведение оперативно-розыскных мероприятий, которые ограничивают конституционные права граждан на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, а также право на неприкосновенность жилища, **допускается на основании судебного решения.**
Подробно:
...в случаях, которые не терпят отлагательств,.. допускается проведение оперативно-розыскных мероприятий ...с обязательным уведомлением суда (судьи) в течение 24 часов. В течение 48 часов с момента начала оперативно-розыскных мероприятий орган, его осуществляющий, обязан получить судебное решение о проведении такого оперативно-розыскного мероприятия либо прекратить его проведение.
Вышеперечисленные положения подкрепляются законом **«О частной детективной и охранной деятельности в Российской Федерации»** (закон № 2487—1 от 11 марта 1992 года). Статья 7 этого закона вводит соответствующие ограничения в сферу деятельности частного детектива. В ней сказано следующее:
Частным детективам запрещается:
>- осуществлять видео- и аудиозапись, фото- и киносъемку в служебных или иных помещениях без письменного согласия на то соответствующих должностных лиц;
>- разглашать собранную информацию, использовать ее в каких-либо целях, вопреки

интересам своего клиента или в интересах третьих лиц.
**>-** проведение сыскных действий, нарушающих тайну переписки, телефонных переговоров и телеграфных сообщений либо связанных с нарушением гарантий неприкосновенности личности или жилища, влечет за собой установленную законом ответственность.
Таким образом, с точки зрения закона только органы, уполномоченные проводить оперативно-розыскные мероприятия, и только на основании судебного решения могут осуществлять негласный сбор информации о физических и юридических лицах. Однако если кто-то из читателей все же решит воспользоваться изложенными сведениями для неблаговидных целей проникновения в чужие секреты, то он должен знать об ответственности за эти деяния. Полезно их знать и в том случае, если вы чувствуете чье-то незримое присутствие в своих делах.
Ниже приведены статьи **Уголовного Кодекса Российской Федерации** (в редакции от 1 января 1997 года), предусматривающие ответственность за информационные преступления.

**Статья 137. Нарушение неприкосновенности частной жизни**

1. Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, если эти деяния совершены из корыстной или иной личной заинтересованности и причинили вред правам и законным интересам граждан, — наказывается штрафом в размере от 200 до 500 минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от 2 до 5 месяцев, либо обязательными работами на срок от 120 до 180 часов, либо исправительными работами на срок до 1 года, либо арестом на срок до 4 месяцев.
2. То же деяние, совершенное лицом с использованием своего служебного положения, — наказывается штрафом в размере от 500 до 800 минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от 5 до 8 месяцев, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от 2 до 5 лет, либо арестом на срок от 4 до 6 месяцев.

**Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений**

1. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан, — наказывается штрафом в размере от 50 до 100 минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период до 1 месяца, либо обязательными работами на срок от 120 до 180 часов, либо исправительными работами на срок до 1 года.
2. То же деяние, совершенное лицом с использованием своего служебного положения или **специальных технических средств, предназначенных для негласного получения информации**, — наказывается штрафом в размере от 100 до 300 минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от 1 до 3 месяцев, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от 2 до 5 лет, либо арестом на срок от 2 до 4 месяцев.
3. Незаконное производство, сбыт или приобретение в целях сбыта **специальных технических средств, предназначенных для негласного получения информации**, — наказывается штрафом в размере от 200 до 500 минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от 2 до 5 месяцев, либо ограничением свободы на срок до 3 лет либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет.

**Статья 139. Нарушение неприкосновенности жилища**

1. Незаконное проникновение в жилище, совершенное против воли проживающего в нем лица, — наказывается штрафом в размере от 50 до 100 минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период до 1 месяца, либо обязательными работами на срок от 120 до 180 часов, либо исправительными работами на срок до 1 года, либо арестом на срок до 3 месяцев.
2. То же деяние, совершенное с применением насилия или с угрозой его применения, — наказывается штрафом в размере от 200 до 500 минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от 2 до 5

месяцев, либо лишением свободы на срок до 2 лет.
3. Деяние, предусмотренное частями первой или второй настоящей статьи, совершенное лицом с использованием своего служебного положения, — наказывается штрафом в размере от 500 до 800 минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от 5 до 8 месяцев, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от 2 до 5 лет, либо арестом на срок от 2 до 4 месяцев, либо лишением свободы на срок до 3 лет.

**Статья 183. Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну**

1. Собирание сведений, составляющих коммерческую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом в целях разглашения либо незаконного использования этих сведений, — наказывается штрафом в размере от 100 до 200 минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от 1 до 2 месяцев, либо лишением свободы на срок до 2 лет.
2. Незаконное разглашение или использование сведений, составляющих коммерческую или банковскую тайну, без согласия их владельца, совершенные из корыстной или иной личной заинтересованности и причинившие крупный ущерб, — наказывается штрафом в размере от 200 до 500 минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от 2 до 5 месяцев, либо лишением свободы на срок до 3 лет со штрафом в размере до 50 минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период до 1 месяца либо без такового.

**Статья 272. Неправомерный доступ к компьютерной информации**

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе в ЭВМ, системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, — наказывается штрафом в размере от 200 до 500 минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от 2 до 5 месяцев, либо исправительными работами на срок от 6 месяцев до 1 года, либо лишением свободы на срок до 2 лет.
2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, — наказывается штрафом в размере от 500 до 800 минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от 5 до 8 месяцев, либо исправительными работами на срок от 1 года до 2 лет, либо арестом на срок от 3 до 6 месяцев, либо лишением свободы на срок до 5 лет.

**Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ**

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами, — наказывается лишением свободы на срок до 3 лет со штрафом в размере от 200 до 500 минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от 2 до 5 месяцев.
2. Те же деяния, повлекшие по неосторожности тяжкие **последствия**, — наказываются лишением свободы на срок от 3 до 7 лет.

**Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети**

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование, модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, — наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет, либо обязательными работами на срок от 180 до 240 часов, либо ограничением свободы на срок до 2 лет.

Те же деяния, повлекшие по неосторожности тяжкие последствия, — наказываются лишением свободы на срок до 4 лет.

**1.2. Основные способы ведения промышленного шпионажа и каналы утечки информации**

За многовековую историю своего развития человечество накопило огромную массу знаний о способах и средствах ведения разведки противоборствующей (конкурирующей) стороны. Естественно, что в основном это опыт военного характера, но он нашел воистину благодатную почву и для мирной реализации на ниве промышленного шпионажа. Рассмотрим основные способы ведения разведывательных (шпионских) действий.

Сбор сведений о фирмах и частных лицах ведется самыми различными способами, но при этом основными каналами утечки информации являются:

>- открытые источники;
>- субъекты — носители информации;
**>-** технические средства разведки.

К открытым источникам относятся каналы, по которым информацию можно почерпнуть без нарушения каких-либо ограничений или запретов:

например, из газет, книг, научных и технических изданий, официальных отчетов и особенно — рекламных каталогов и брошюр. Подобным образом работает большинство разведок мира. Понятно, что основная работа при этом ложится на специально подготовленных аналитиков, которые пропускают через себя горы материалов, отсеивая все ненужное и постепенно накапливая необходимые сведения. Главными объектами такого анализа для получения конфиденциальной информации являются:

>- доклады на конференциях, симпозиумах и т. д.;
>- вопросы, осторожно задаваемые специалистами;
>- попытки пригласить на работу сотрудников конкурирующей формы и заполнение ими при этом специальных вопросников;
**>-** прием на работу, обычно с резким увеличением оклада, служащего конкурирующей фирмы (своего рода законный подкуп);
>- изучение выставочных образцов;
**>-** притворные переговоры с конкурентами о приобретении лицензии или совместной деятельности и т. д.

Все эти методы давно опробованы на Западе. По мере становления служб безопасности крупных коммерческих организаций и создании при них серьезных аналитических отделов, при условии привлечения специалистов из разведки, легальные источники сбора информации и в России займут подобающее им место в системе сбора данных.

Перекрытие легальных каналов утечки — чрезвычайно сложная и трудоемкая задача. Подробно на этих вопросах мы останавливаться не будем. Скажем только о главном правиле — всегда нужно помнить о свойстве информации постепенно накапливаться. Поэтому, когда вы даете внешне безобидную рекламу или интервью, посылаете отчет или делаете доклад, всегда сопоставляйте их содержание с ранее «засвеченными» материалами, в сочетании с ними ваши откровения могут иметь совсем другое значение. И последнее, хотя при отсутствии серьезной цензуры собирать открытую информацию довольно легко, но не менее легко дать по этому каналу и дезинформацию. По этой причине тайный сбор сведений еще долго будет оставаться важным видом деятельности как для государственных структур, так и для некоторых категорий граждан.

Использование субъектов — носителей информации — пожалуй, самый древний способ шпионажа. В ряду источников конфиденциальной информации люди занимают особое место, ибо способны выступать не только обладателями неких сведений, но и субъектами злонамеренных действий. Действительно, в отличие от технического устройства их можно подкупить или шантажировать. Притом, люди являются обладателями и распространителями информации не только в пределах своих функциональных обязанностей, их возможности гораздо шире. Помимо простого обладания набором сведений они способны их анализировать, обобщать и делать выводы. То есть получать требуемую информацию и по совокупности косвенных данных. На деяния такого рода пока не способна никакая суперЭВМ. При определенных условиях люди способны скрывать, воровать, продавать информацию и совершать иные криминальные действия вплоть до вступления в устойчивые преступные связи со злоумышленниками.

Наиболее разностороннюю и полезную информацию о какой-нибудь организации удается получить, завербовав ее сотрудника либо внедрив туда своего человека. Внедрить можно как сотоварища, так и наемного специалиста. Существует два способа внедрения:

>- под собственным именем;
>- с фиктивными документами и легендой.

Различают три уровня внедрения:

>- тихое присутствие на общих сборах в качестве стороннего наблюдателя;
>- некое участие в делах разрабатываемой организации;
>- целевой проход в руководящее звено.
Для внедрения прибегают к следующим приемам:
>- заведение знакомства с сотрудником организации, который по цепочке передает внедряемого руководству;
>- выход самому на руководство с предложением перспективного дела, обоснованием своей полезности, сообщением важной информации;
>- предъявление реальных или сфабрикованных рекомендаций;
>- афиширование «измены» конкурентам;
>- использование затруднений организации в работе с эффективным оказанием им неожиданной помощи;
>- побуждение организации самой искать контакт с подставленным человеком. За счет распространения в определенной среде слухов о каких-то необычных возможностях или познаниях объекта, которые способны помочь в решении конкретных проблем;
>- опубликование статьи в СМИ или выпуск брошюры созвучного, сочувственного или рекламного содержания, и использование ее как пропуск для проникновения в интересующие структуры (хотя бы на первый уровень) и т. д.
Однако осуществить внедрение в устоявшуюся организацию весьма проблематично, поэтому чаще всего прибегают к вербовке уже действующих сотрудников. Ясно, что чем выше уровень завербованного человека, тем шире у него возможности, и тем большую ценность он представляет, но некоторую пользу может дать привлечение на свою сторону даже вспомогательного персонала. Поэтому нельзя пренебрегать никакой возможностью «зацепиться» за штатного сотрудника из «разрабатываемой» организации.
Наиболее выгодны для вербовки те, кто:
>- обладают некими моральными изъянами (страстью к алкоголю, наркотикам, женщинам...);
>- имеют долги или денежные затруднения;
>- по каким-то причинам (неудача в карьере, неурядицы в личной жизни, взгляды на проводимую политику...) сильно раздражены или озлоблены.
Правда, процесс выявления кандидата в агенты является достаточно сложным. Вначале проводится оценка и разработка потенциального кандидата, под чем понимается изучение его личных качеств и способностей, а также изыскание способов его наиболее эффективной вербовки и использования. Далее производится знакомство с объектом, его тщательное изучение и при обнаружении «зацепок» сама вербовка на почве шантажа, подкупа, идейных соображений, личного неприятия руководителя кампании и т. д. Чтобы читатель имел представление об этом процессе, расскажем более подробно о каждом из этапов.
Знакомство связано с созданием благоприятной ситуации, многие из коих могут возникнуть совершенно случайно, и здесь главное — не упустить свой шанс. Если такой ситуации ждать нет времени, то существует множество приемов, которые обеспечивают оптимальный повод для начального обмена фразами:
>- провоцирование на оказание помощи (симуляция падения, тяжелые вещи в руках, сломанная машина и т.д.) — обычно, это женский вариант;
>- предложения себя объекту в качестве необходимого ему в данный момент компаньона (игра в карты, шахматы или распитие на троих...);
>- знакомство через общих знакомых;
>- знакомство в очередях и транспорте;
>- знакомство на основе хобби;
>- знакомство через детей и т. д.
Главное — помнить правило, что внешне инициатива знакомства должна исходить от объекта, а задача вербовщика эту инициативу только разжечь. Первый контакт надо заканчивать вежливой, но не обязывающей фразой «как-нибудь созвониться». После этого надо создать повод для «случайной» повторной встречи в театре, на улице, вечеринке и т. д. Затем можно углубить контакт, раскрывшись перед объектом со стороны, вызывающей у него благоговейное восхищение. Например, для женщины показать потрясающее умение и храбрость при инсценировке криминального нападения. Или наоборот, поплакаться о своих неприятностях, но не переборщить. После углубления знакомства вербовщик старается как можно чаще общаться с объектом, чтобы составить

о нем возможно более полное представление.
Уяснив в ходе общения психологический портрет объекта и оценив его натуру, обычно удается выйти на мотивы, способные склонить намеченного человека к сотрудничеству, оценить его реальную уязвимость. Чаще всего ими являются:
>- политические или религиозные убеждения;
>- национализм;
>- преувеличенное мнение о своих способностях;
>- месть шефу;
>- материальные затруднения;
>- страх компрометации;
>- жадность;
>- любовь-страсть;
>- житейские слабости и пороки.
Вербовку можно вести от имени организации, под чужим флагом, без непосредственного указания, кто вербует. Очень часто агенту неизвестно, на кого он работает, либо ему дается неверная информация. Позднее, когда приобретут силу финансовые или другие средства контроля, завербованному, часто к его ужасу, раскрывают истинное имя хозяина. Впрочем, как показал богатый опыт спецслужб, более эффективной работы от агента можно добиться путем убеждения, а не угроз, и умные хозяева стремятся развивать дружеские отношения с ним.
Завербовав конкретного человека, стараются получить от него максимум пользы, а это удается лишь при умелом руководстве, учитывающем психологические особенности личности и уровень желания (или нежелания) действовать. Частота использования зависит от оперативной необходимости и степени доверенной ему инициативы. Агент может функционировать:
>- независимо (сам решать, какую информацию и когда передавать);
>- автономно (работать по установленному заданию);
**>-** строго по инструкции.
Финансовое вознаграждение при взаимодействии является своего рода подпитывающим фактором, превосходящим все прочие стимулы. Оно должно быть хорошо продумано, чтобы не оскорблять самолюбие, заметно зависеть от полезности работы и быть достаточно большим, чтобы не перекупили другие. Немаловажно также создать у агента впечатление о значимости его работы с моральной и идеологической точки зрения.
Думаем, что прочитав этот краткий и, конечно же, поверхностный материал, руководитель организации сотни раз подумает, прежде чем брать на более-менее ответственную должность человека с подмоченной репутацией или с характеристикой типа «отличный специалист, но бабник или любитель выпить», даже при наличии весьма солидных рекомендаций. Следует также контролировать свой «бурный» темперамент, и не в коем случае не оскорблять подчиненных, а тем более не создавать в фирме плохой психологический климат. Очевидно, что этим создается очередное слабое звено в системе безопасности организации.
Обнаружение скрытого агента — очень сложная и трудоемкая задача, требующая специальных навыков оперативной работы. Останавливаться на этих вопросах мы не будем, поскольку все материалы по методам ведения оперативной работы являются сугубо секретными, да и данная тематика выходит за рамки как нашей книги, так и нашей квалификации. Отметим только, что при правильной организации деятельности фирмы большинство агентов (особенно обслуживающий персонал) не может обладать всей полнотой информации. В этом случае их используют для легального проникновения в помещения с целью установки подслушивающих устройств и исследования содержимого мусорных корзин.
Для некоторого затруднения деятельности таких агентов необходимо:
>- определить строгий порядок и выделить специально оборудованные помещения для ведения деловых бесед, чтобы исключить даже кратковременное «случайное» присутствие посторонних, в том числе и из числа своих сотрудников;
>- организовать максимально жесткий учет и строго регламентировать порядок работы с деловыми документами;
**>-** узаконить и максимально ограничить круг лиц, допускаемых к тем или иным внутрифирменным секретам;
**>-** запретить сотрудникам вести служебные переговоры с домашних телефонов;

>- в деловых беседах исходить всегда из того предположения, что ваш телефон прослушивается, особенно если это радиотелефон;
**>-** относиться крайне осторожно к лицам, выдающим себя за работников городских коммунальных служб или ремонтников;
>- при посторонних нельзя называть фамилию и имя-отчество собеседника, а назначая место встречи надо переходить на условности и т. д.
Но эти меры будут недостаточными, если нельзя исключить применение «доброжелателями» технических средств несанкционированного съема информации. Наличие специальной аппаратуры способно резко увеличить деловой потенциал разведчика в любой сложной игре. Официальная продажа таких вещичек ограничена, но на диком рынке можно легко найти как фирменные образцы, так и топорные поделки отечественных «умельцев». Незаменимым подспорьем могут стать и некоторые образцы бытовой радиоаппаратуры. Например, уникальными возможностями для подслушивания радиопереговоров обладает радиотелефон «Алтай», выпускаемый местным заводом в белорусском городе Молодечно. Впрочем, на практике очень часто обходятся довольно примитивными средствами вполне самостоятельного изготовления, особенно если финансовые возможности весьма ограничены, а со стороны объекта отсутствуют даже признаки каких-либо мер по обеспечению технической безопасности. Общая характеристика основных методов получения информации о различных сторонах деятельности и перечень используемых при этом технических средств приведены в табл. 1.2.1.

**Таблица 1.2.1. Технические средства, предназначенные для получения конфиденциальной информации**

№ п/п /Действия /Физическое явление /Способ (средство) съема информации
1 /2 /3 /4

1 /Разговор нескольких лиц /Акустический сигнал /Подслушивание, в том числе случайное Диктофоны Закладные устройства с передачей информации по: Имеющимся коммуникациям (трубам, цепям сигнализации, сетям 220 В, телефонным линиям...); специально проложенным проводам; радио- или ИК-каналу Направленный микрофон

//Виброакустический сигнал /Стетоскоп Вибродатчик с передачей информации по: радиоканалу; проводам; коммуникациям; ИК-каналу Оптический лазерный микрофон

//Гидроакустический сигнал /Гидроакустический датчик

//Акустоэлектрический сигнал /Радиоприемник спецназначения

//Движение губ /Визуально, в том числе оптическими приборами Камера, в том числе с передачей по проводам и радиоканалу

2 /Разговор по телефону /Акустический сигнал /Аналогично п. 1

//Электрический сигнал в линии /Параллельный телефон, прямое подключение, подключение через электромагнитный датчик, телефонная радиозакладка

//Побочные электромагнитные излучения (ПЭМИ) и наводки /Специальные радиотехнические устройства

Окончание табл. 1.2.1

№ п/п /Действия /Физическое явление /Способ (средство) съема информации
1 /2 /3 /4

3 /Разговор по радиотелефону /Акустический сигнал Электромагнитные волны /Аппаратура п. 1 Специальные радиоприемные устройства

4 /Документ на бумажном носителе /Наличие /Визуально, в том числе с помощью оптических средств Фотографирование, в том числе с дистанционной передачей снимка Копирование

5 /Размножение документа на бумажном носителе /Следы на нижнем листе, копировальной бумаге или красящей ленте /Кража, визуально

//Шумы принтера /Спецаппаратура акустического контроля

//ПЭМИ от ЭВМ /Специальные радиотехнические устройства

6 /Почтовые отправления /Наличие /Прочтение: со вскрытием, без вскрытия

7 /Документ на небумажном носителе /Носитель /Копирование, вскрытие, несанкционированное использование ЭВМ

8 /Изготовление документа на небумажном носителе /Изображение на дисплее

/Визуально, в том числе с помощью оптических средств Фотографирование Видео- или телевизионные закладные устройства

//ПЭМИ /Специальные радиотехнические устройства

//Электрические сигналы в сетях /Аппаратные закладки

9 /Передача документа на небумажном носителе /Электрические сигналы /Несанкционированное подключение, имитация пользователя

Таблица содержит лишь самые общие данные. Подробно о каждом из перечисленных в ней средств можно узнать из материалов первой части книги.

### 1.3. Средства перехвата аудиоинформации

#### 1.3.1. Закладные устройства с передачей информации по радиоканалу

**Общие сведения о закладных устройствах**

Один из эффективных путей негласного получения коммерческой информации основан на применении так называемых закладных устройств (ЗУ), скрытно устанавливаемых в местах возможного нахождения объектов наблюдения (конкурентов) либо подключаемых к используемым ими каналам связи.

В настоящее время создано огромное количество типов таких устройств, различающихся принципом функционирования, способом передачи информации, дальностью действия, а также размером и внешним оформлением.

Так, самые миниатюрные ЗУ имеют вес всего 1,5 г и линейные размеры — не более нескольких миллиметров. Дальность передачи информации с таких устройств едва превышает 10 м. Более мощные устройства имеют размеры до нескольких сантиметров и позволяют осуществить передачу перехватываемой информации на дальность от нескольких сот до тысячи и более метров. Обычно ЗУ скрытно устанавливаются в элементах конструкций зданий и интерьера, крепятся под одеждой или камуфлируются под личные вещи.

Для того чтобы систематизировать представление о таких устройствах, целесообразно ввести пять признаков их классификации (рис.1.3.1):

>- по каналу передачи информации;
>- по способу восприятия информации;
>- по наличию устройства управления;
>- по внешнему виду;
>- по используемому источнику питания.

Рассмотрим отдельно каждый из признаков. В зависимости от канала передачи информации различают следующие типы ЗУ (рис.1.3.2):

**>-** радиозакладки;
>- инфракрасные закладки;
>- закладки с передачей информации по токоведущим линиям;
>- закладки с записью на магнитофон.

В радиозакладках для передачи информации используется энергия электромагнитных волн, не влияющих на органы чувств человека, способных распространяться на значительные расстояния, преодолевая естественные

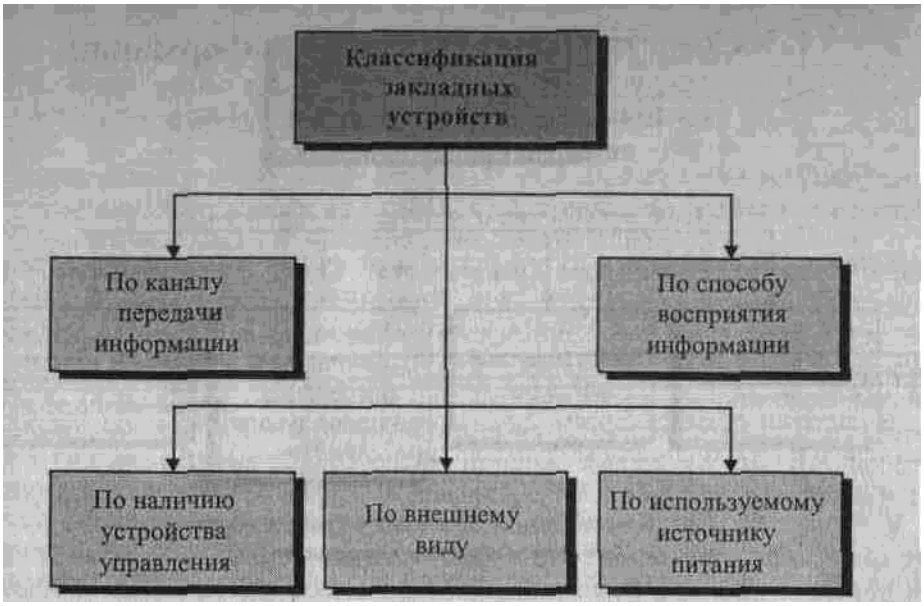



**Рис. 1.3.1. Основные признаки классификации закладных устройств**

и искусственные препятствия. Благодаря этим двум свойствам радиозакладные устройства позволяют с помощью специальной приемной аппаратуры вести скрытное наблюдение за интересующим объектом практически из любой удаленной точки.

С технической точки зрения, закладки могут работать практически в любом диапазоне радиоволн. Однако из конструктивных соображений наиболее используемые частоты — от 100 до 1000 МГц. Более подробно этот вид ЗУ будет рассмотрен ниже. В инфракрасных закладках для передачи информации также используется энергия электромагнитных волн, но не радиодиапазона, а невидимой части оптической области спектра — инфракрасного диапазона.

Благодаря малой длине такие волны распространяются узким пучком в заданном направлении, и их трудно обнаружить даже с помощью специальной аппаратуры. Дальность передачи информации от инфракрасных ЗУ достигает 500 м.

Однако высокая скрытность таких устройств существенно усложняет их применение. Так, инфракрасная закладка должна постоянно находиться в зоне прямой видимости приемника оптического излучения, а случайно попавший на линию визирования предмет, человек или автомобиль, а также изменившиеся погодные условия могут привести к существенному ухудшению качества или даже пропаданию сигнала в аппаратуре регистрации. Естественно, что такие ЗУ совершенно не применимы на мобильных объектах.


**Рис. 1.3.2. Классификация закладных устройств в зависимости от канала передачи информации**

В силу перечисленных недостатков инфракрасные закладки не нашли широкого использования в практике промышленного шпионажа.

Закладки с передачей информации по токоведущим линиям используют свойство электрических сигналов распространяться на значительные расстояния по проводникам. Такие ЗУ обладают существенными достоинствами: высокой скрытностью передачи информации, большой дальностью действия, отсутствием необходимости в дополнительных источниках питания. Кроме того, они хорошо камуфлируются под элементы электрических цепей и токоприемники (розетки, тройники, электрические удлинители, настольные лампы и т. д.). В качестве токопроводящих линий используются либо специально проложенные провода, либо кабели электрических и телефонных сетей. В силу перечисленных обстоятельств ЗУ такого типа часто применяются недобросовестными конкурентами для получения сведений конфиденциального характера. Более подробно они будут рассмотрены в п. 1.3.2.

В случаях, когда отсутствует необходимость получения оперативной информации в реальном масштабе времени, а также имеется возможность скрытного извлечения и замены кассеты или магнитной ленты, закладка может оснащаться магнитофоном вместо устройства передачи по одному из рассмотренных каналов.

Такой способ, как правило, применяется только в тех случаях, когда есть потенциальная угроза обнаружения объектом наблюдения канала передачи информации (например, с помощью специальной аппаратуры контроля).

В зависимости от **способа восприятия информации** различают три типа ЗУ (рис.1.3.3):

>- микрофонного типа;
>- вибрационного типа;
>- с подключением к коммуникационным линиям.

Принцип действия ЗУ микрофонного типа основан на **преобразовании** акустических атмосферных колебаний в электрические сигналы и **передаче** их потребителю одним из вышеперечисленных способов.

ЗУ вибрационного типа (стетоскопы) перехватывают акустические колебания твердых сред (вибрации), возникающие вследствие давления атмосферных акустических волн на среды (рис. 1.3.4). В качестве чувствительных элементов в таких устройствах обычно используются пьезомикрофоны, электронные микрофоны или датчики акселерометрического типа. Они наиболее эффективны при фиксации на тонких «площадных» поверхностях (межкомнатных перегородках, стеклах, дверях и т. п.). Для передачи информации потребителю, как правило, используется радиоканал, и такие ЗУ обычно называют радиостетоскопами.

ЗУ с подключением к коммуникационным линиям предназначены для негласного перехвата информации, циркулирующей в телефонных или волоконно-оптических линиях.

Они позволяют скрытно получать информацию о содержании телефонных переговоров, а также текстовых сообщений (телеграфных, факсимильных, электронной почты и т. д.).

Для передачи информации с подключаемых ЗУ обычно используется радиоканал, а такие устройства называются радиозакладными. По способу подключения к телефонным линиям радиозакладки делят на две группы (рис. 1.3.5).

Первая группа — радиозакладки с непосредственным подключением.

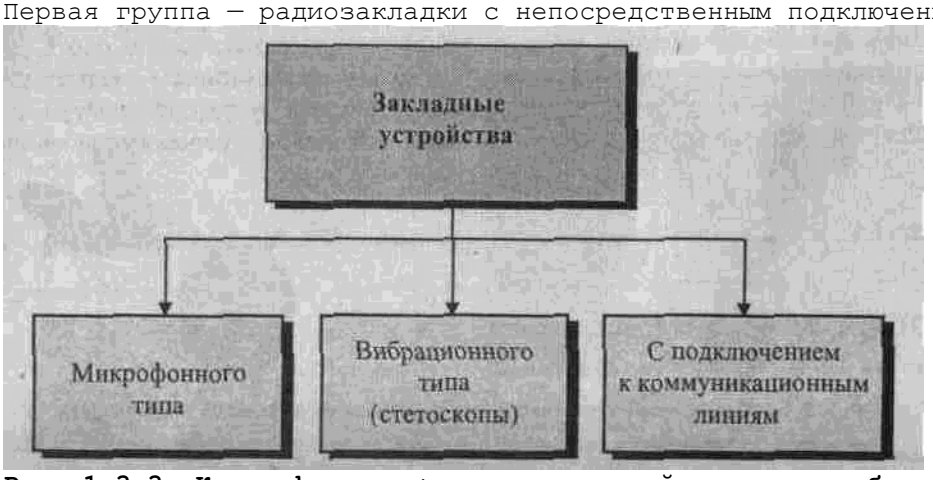



**Рис. 1.3.3. Классификация закладных устройств по способу восприятия информации**

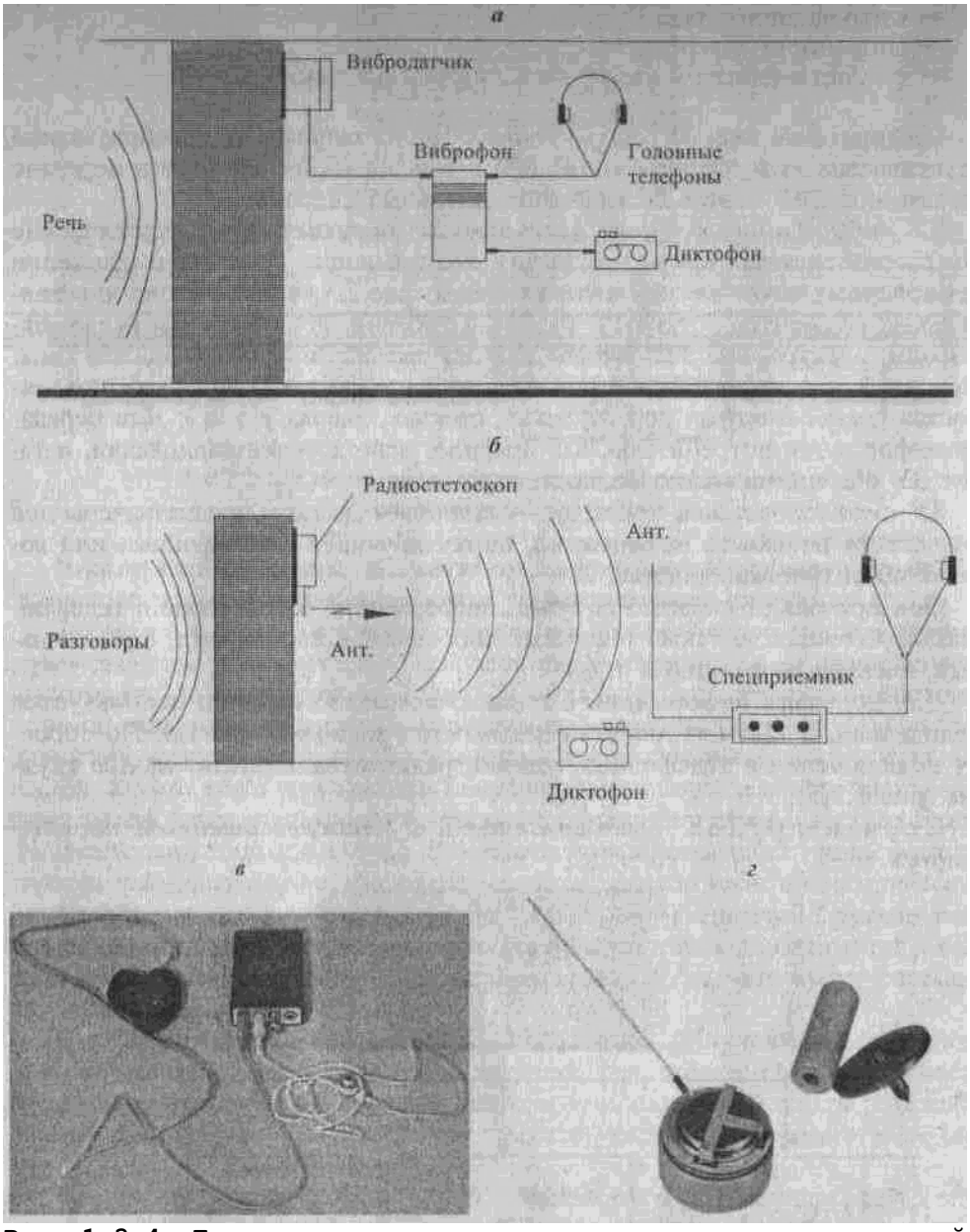



**Рис. 1.3.4. Применение стетоскопов для перехвата акустической информации:**
а — с передачей информации по специально проложенным проводным линиям; б — с передачей по радиоканалу; в — внешний вид стетоскопа с передачей информации по проводам; г — стетоскоп с передачей по радиоканалу

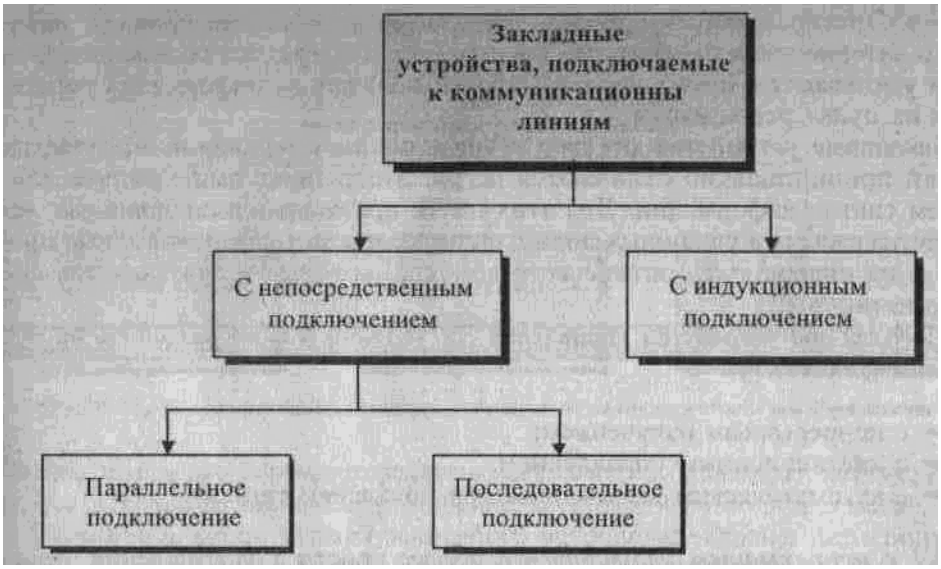



**Рис. 1.3.5. Классификация радиозакладных устройств по способу подключения к токопроводящим коммуникационным линиям**

Они подключаются либо одновременно к обоим проводам параллельно абоненту (параллельное подключение — рис. 1.3.6, а), либо в разрыв одного из проводов (последовательное подключение — рис. 1.3.6, б).

Такие способы позволяют получить достаточно большой уровень сигнала (его хорошее качество) на входе радиозакладки, а также обеспечить ее питание от линии. Однако закладки с непосредственным подключением могут быть легко обнаружены по изменению параметров линии.

Этого недостатка в значительной степени лишены устройства второй группы— радиозакладки с индукционным подключением (рис.1.3.6, в). В таких закладках чувствительным элементом выступает специальным образом построенная антенна, устанавливаемая вплотную к проводам телефонной

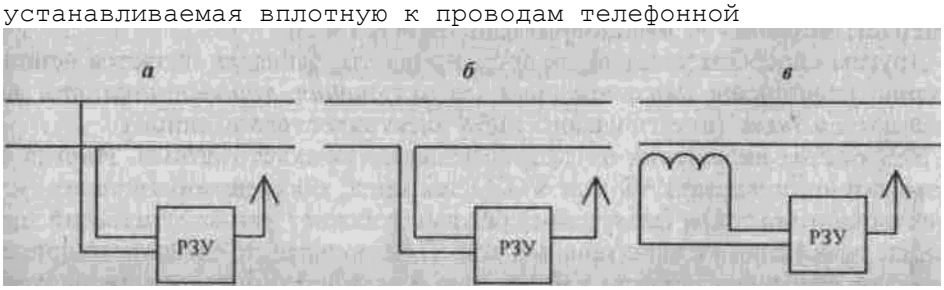



**Рис. 1.3.6. Виды подключения радиозакладных устройств к токопроводящим линиям: а — параллельное; б — последовательное; в — индукционное**

линии. Электромагнитное поле, окружающее телефонные провода, наводит в антенне токи, содержащие информацию о характере сообщения. Эти токи усиливаются, преобразуются и далее полученная информация передается на пункт регистрации.

Закладные устройства для снятия информации с волоконно-оптических линий принципиально отличаются от рассмотренных выше только способом снятия информации. Для этих целей применяются специальные устройства сжатия волоконных линий, вызывающие интерференционные процессы на поверхности оптического волокна, которые и считываются фотоприемником.

По **наличию устройства управления** ЗУ условно можно разделить на три группы (рис.1.3.7):

>- с непрерывным излучением;
>- с дистанционным управлением;
>- с автоматическим включением при появлении сигнала.

ЗУ с непрерывным излучением наиболее просты в изготовлении, дешевы и предназначены для получения информации в течение ограниченного промежутка времени. Работа на излучение таких ЗУ начинается с момента подключения питания. Если источник питания автономный, то, как правило, время работы такого ЗУ не превышает 1—2 часа из-за

большого потребления энергии на передачу сигнала. Время работы ЗУ, питающихся от линий (силовых или телефонных), практически неограничено.
Однако общим существенным недостатком для всех ЗУ с непрерывным излучением является возможность их обнаружения по излучению.
Существенно увеличить время непрерывной работы устройств с автономным питанием и повысить скрытность позволяет применение дистанционного управления ЗУ. Оно позволяет переводить устройство в режим излучения только в тех случаях, когда объект наблюдения ведет переговоры либо передает информацию по каналам связи.
Время излучения может быть дополнительно сокращено, если закладка содержит устройство накопления и сжатия сигнала.
Другим способом увеличения времени работы закладки является использование устройств автоматического включения передатчика при появлении сигнала (акустического либо электрического в линии).
Устройства включения от голоса называются акустоматами. Иногда их называют системами VAS или VOX. Закладка, оборудованная таким устройством, в обычном (дежурном) режиме работает как акустический приемник, потребляя незначительный ток. При появлении сигнала, например в начале разговора объекта наблюдения с кем-либо, подается напряжение на передатчик, и тот переходит в режим излучения. При пропадании акустического сигнала (прекращении разговора) через определенное время,

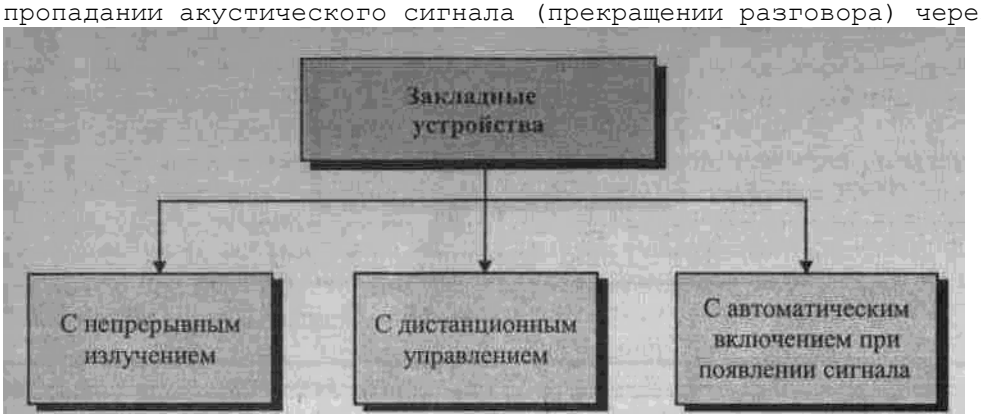



**Рис. 1.3.7. Классификация закладных устройств по наличию устройства управления**

обычно несколько секунд, передатчик выключается и закладка переходит в режим дежурного приема. Применение акустомата позволяет в несколько раз увеличить время работы закладного устройства. Однако их использование приводит к потере первых слов при каждом включении.
По **используемому источнику питания**, как было отмечено выше, ЗУ делятся на два вида (рис.1.3.8):
>- с собственным источником;
>- с питанием от внешнего источника.
К первому виду относятся любые ЗУ, имеющие собственный встроенный аккумулятор.
Ко второму — ЗУ с передачей информации по токоведущим линиям и ЗУ с непосредственным подключением к коммуникационным линиям. Время работы этих устройств практически неограничено.


**Рис. 1.3.8. Классификация закладных устройств по используемому источнику питания**


**Рис. 1.3.9. Классификация закладных устройств по внешнему виду**

**По внешнему виду ЗУ** могут быть (рис. 1.3.9):

>- в обычном исполнении;
>- в закамуфлированном виде.

В обычном исполнении устройства имеют, как правило, металлический корпус (окрашенный или нет) и форму параллелепипеда. Они достаточно универсальны и применяются в различных условиях обстановки. Маскируются одеждой, предметами интерьера (корзиной для бумаг, пластиковой коробкой, книгами, картиной и т. п.) либо местными предметами, пропускающими акустические и (или) электромагнитные колебания (травой, смятым бумажным либо пластиковым пакетом, куском доски, фанеры и т. п.).

В закамуфлированном виде ЗУ применяются только в соответствии с конкретной обстановкой. Так, например, в виде силовой или телефонной розетки только в том случае, если другие неиспользуемые розетки в помещении имеют такой же внешний вид, в виде личных вещей (часов, зажигалки, заколки...), если они соответствуют общему имиджу применяющего их человека.

Возможные варианты внешнего вида серийно выпускаемых закладных устройств приведены ниже, в табл. 1.3.1...1.3.3.

**Радиозакладки**

Наиболее широкое применение в практике промышленного шпионажа нашли устройства с радиоканалом передачи перехватываемой информации, так называемые радиозакладные устройства (РЗУ), или радиозакладки.

Повышенный интерес к использованию РЗУ связан с их исключительно широкими возможностями по наблюдению за мобильными объектами, находящимися на значительном расстоянии.

Радиозакладные устройства как радиотехнические средства обладают рядом специфических особенностей, не свойственных другим ЗУ. В соответствии с этими особенностями для классификации радиозакладок могут быть использованы следующие признаки (рис. 1.3.10):

>- принцип формирования сигнала;
>- способ закрытия передаваемой информации;
>- дальность действия.

В соответствии с **принципом формирования сигнала** (рис. 1.3.11) РЗУ могут быть:

>- активные;
>- пассивные;
>- полуактивные.

Активные РЗУ наиболее распространены. В общем виде они могут быть представлены структурной схемой, изображенной на рис. 1.3.12.

Описание внешнего вида и основных характеристик некоторых активных РЗУ приведены в табл. 1.3.1.

Полуактивные РЗУ характеризуются существенно большим временем функционирования от автономного источника питания: до 4000 часов. Положительный эффект достигается за счет комплексного использования энергии внешнего специально сформированного мощного зондирующего сигнала и энергии собственного питающего элемента. При этом энергия


**Рис. 1.3.10. Признаки классификации радвозакладок**

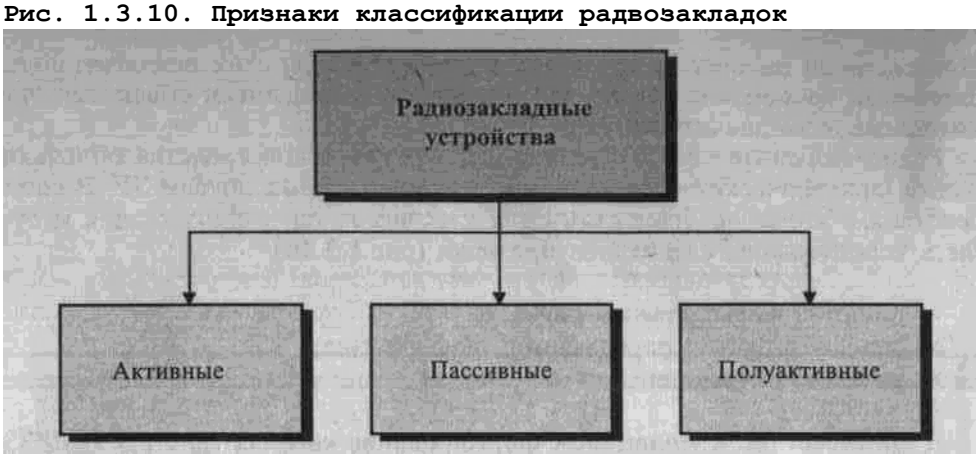



**Рис. 1.3.11. Классификация радиозакладок по принципу формирования сигнала**

собственного аккумулятора тратится лишь на модуляцию принимаемого высокочастотного сигнала и его усиление.

Так как такие радиозакладки могут работать только при наличии внешнего зондирующего электромагнитного поля, то они получили название «аудио-транспондеры» («аудиоответчики») от английского audiotransponder. Структурная схема полу активного РЗУ показана на рис. 1.3.13. Примером аудиотранспондеров могут служить радиозакладки SIM-ATP-16 и SIM-ATP-40 (табл. 1.3.2).

**SIM-ATP-16** — аудиотранспондер, имеющий размеры 90'90'4 мм, выглядит подобно дискете 3,5". Его легко можно спрятать в интерьере комнаты. Устройство упаковано в фольгу и может храниться более двух лет. Для приведения в рабочее состояние фольга должна быть снята и на расстоянии не более 10 м (в соседней комнате или автомобиле) должен быть установлен генератор синусоидального сигнала мощностью 10 Вт с частотой излучения 160 МГц.

Схемой РЗУ предусмотрено, что переизлученный сигнал сдвинут относительно зондирующего на +12 кГц. Это обеспечивает развязку приемного и передающего каналов и маскировку полезного маломощного сигнала сильным зондирующим. Информационный сигнал может быть принят специальным приемником на удалении до 500 м. Для приема и переизлучения сигналов используется плоская кольцевая антенна.

Однако мощный зондирующий сигнал является демаскирующим признаком применения полуактивного ЗУ, что для руководителя службы безопасности должно послужить толчком к проведению соответствующих мероприятий по защите информации.

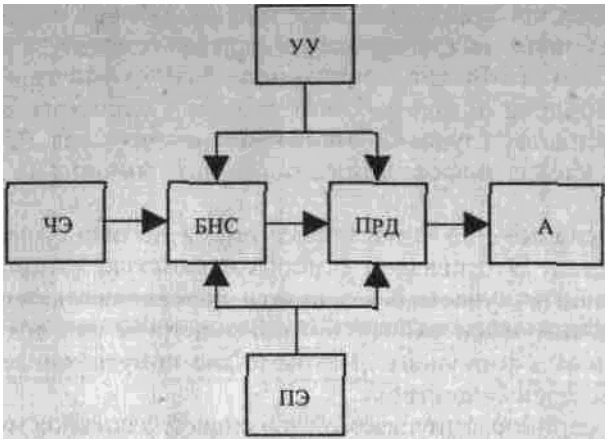
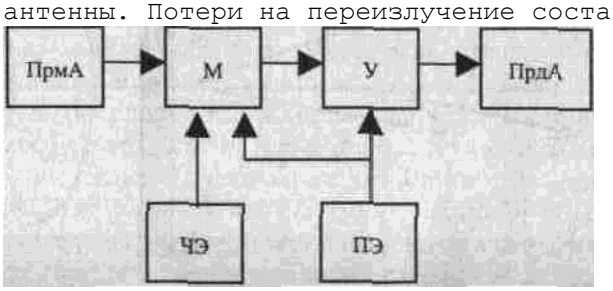



**Рис. 1.3.12. Типовая структурная схема активного радиозакладного устройства:**
УУ — устройство управления (например, акустомат или приемник сигналов от блока дистанционного управления); ЧЭ — чувствительный элемент (микрофон, вибродатчик или специальная антенна для перехвата электромагнитных полей коммуникационных линий и т. п.); БНС — блок накопления и сжатия информации, предназначенный для уменьшения времени работы РЗУ на излучение (до нескольких секунд за сеанс передачи); ПРД — передатчик, работающий на частотах, лежащих в диапазоне 100...1000 МГц; А — антенна (как правило, встроенная либо в виде отрезка изолированного провода длиной. 1=1/4, где 1 — длина волны излучения); ЛЭ — питающий элемент (может отсутствовать, если РЗУ подключено к линии, находящейся под напряжением)

**SIM-ATP-40** — отличается от SIM-ATP-16 тем, что имеет габариты 130x75x250 мм и работает в диапазоне 800...950 МГц. Необходимая мощность облучающего сигнала лежит в пределах от 0,1 до 20 мВт. Дальность активации системы передатчиком — 10 м. Время работы транспондера от внутренней батареи напряжением 3 В — до 4 месяцев. Для облучения и приема переизлученного сигнала используются направленные директорные антенны. Потери на переизлучение составляют около 8 дБ.




**Рте. 1.3.13. Типовая структурная схема полуактивного раднозакладного устройства ПрмА и ПрдА — приемная и передающая антенны, соответственно; М — модулятор; У — усилитель**

Принцип действия пассивных РЗУ был разработан еще в середине 40-х годов. Одна из таких радиозакладок в течение многих лет проработала в посольстве США в Москве, спрятанная в гипсовый герб Соединенных Штатов, установленный над рабочим столом в кабинете посла. Выявлена она была с большим трудом и только после того, как ЦРУ стало точно известно, что утечка информации происходит именно из этого кабинета (см. п.1.3.5).

Однако пассивные РЗУ в настоящее время не нашли достаточно широкого применения. Это связано с необходимостью использования столь высоких уровней излучаемой мощности передатчиков, что обслуживающий персонал вынужден работать с применением защитных средств (например, свинцовых фартуков). В этом плане полуактивные РЗУ обладают существенным преимуществом.

Примером серийно выпускаемой пассивной закладки может служить

**SIPE MM1** — пассивная радиозакладка, выполненная в виде стержня длиной около 30 см и диаметром 2,5 см. Дальность действия — 100 м. Поставляется в комплекте, состоящем из закладки, источника облучения с питанием от электросети и приемного устройства.

Принцип применения пассивных и полуактивных радиозакладок иллюстрируется на рис. 1.3.14.

**По способу закрытия информации,** передаваемой в радиоканале, РЗУ делятся на три вида (рис. 1.3.15):

>- без закрытия информации;
>- с использованием сложных видов модуляции;
>- с кодированием информации.

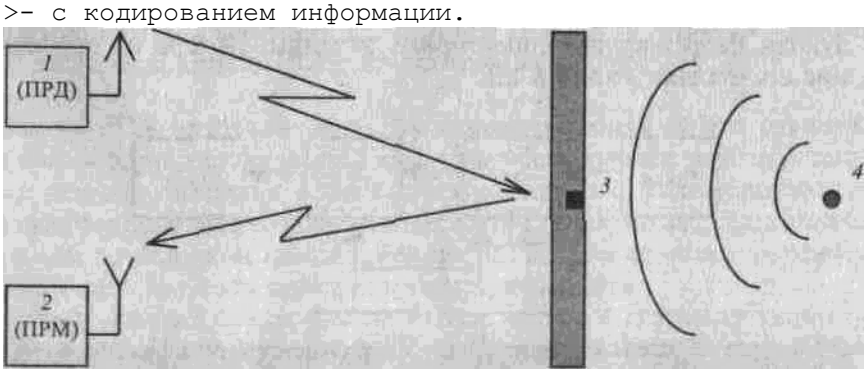



**Рис. 1.3.14. Схема применения полуактивной и пассивной радиозакладок:**
**1, 2 - передатчик и приемник, настроенные на частоту работы закладного устройства;**
**3 - полуактивная либо пассивная радиозакладка; 4 - источник акустического сигнала**

**Таблица 1.3.1. Основные характеристики активных радиозакладных устройств**

| Вид исполнения | Индекс | Частота, МГц<br>Вид модуляции | Вых. мощн., мВт<br>Дальн. действия, м | Габариты, мм<br>Масса, г | Тип антенны<br>Питание, В | Время работы, ч | Примечание |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Обычный | STG 4007 | 395, 41<br>Узкополосная частотная | 15<br>150 | 66×27×14<br>52 г | Гибкая | | Акустомат |
| Обычный | PK1380 -S | 115...200<br>Узкополосная частотная (±5 кГц) | 40 | 33×33×20 | Гибкая<br>9 | 10 | Кварцевая стабилизация частоты.<br>Кодирование сигнала (инверсия спектра) |
| Обычный | SIM-PR-9000T | 350...450<br>Широкополосная частотная ( 5 МГц) | 100 | 70×39×5<br>51 | Встроенная<br>6...10 | | Двухканальный режим работы. Цифровое кодирование сигнала |
| Обычный | PK1195 -SS | 427<br>Узкополосная частотная (±5 кГц) | 1...100 | 20×55×5 | | | Дистанц. управление. Акустомат (VOX).<br>Цифровой сигнал с кодированием |
| Обычный | PK540-SS | 427<br>Узкополосная Частотная (±5 кГц) | 20 | 65×50×30 | Гибкая<br>9 | 10 | Кварцевая стабилизация частоты.<br>Кодирование сигнала |
| Обычный | PK1970 - SS | 427<br>Двойная модуляция | | 80×50×20 | Гибкая<br>9; 220 | | |

**Продолжение табл. 1.3.1.**

| Вид исполнения | Индекс | Частота, МГц<br>Вид модуляции | Вых. мощн., мВт<br>Дальн. действия, м | Габариты, мм<br>Масса, г | Тип антенны<br>Питание, В | Время работы, ч | Примечание |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Обычный | РК1970 | 427<br>Широкополосная частотная | 10/100 | 70×47×9 | Гибкая<br>6...10 | | Цифровой скремблированный сигнал |
| Обычный | РК2050 | 1,3 ГГц<br>Частотная | 10 | | Гибкая<br>220/110 | | Цифровой сигнал |
| Деревянный брусок | «Брусок-ЛЗБ ДУ» | 415...425<br>Частотная | ——<br>300 | | Встроенная | 25 суток | Дистанционное управление. Кварц. стабил. частоты. Кодирование сигнала (сложная инверсия спектра) |
| Лист упаковочного гофрокартона | «Картонка ДУ» | 300<br>Узкополосная частотная | 0,5...20<br>50...250 | 6×10÷70 см$^3$ | | 50...400;<br>3...12 мес. в дежурном режиме | Дистанционное управление (500 м на $f$ = 140...170 МГц). Кварцевая стабилизация частоты |
| Папка для документов | «Папка ДУ» | 300<br>Узкополосная частотная | 0,5...50<br>50...500 | | | 20...500,<br>3...12 мес. в дежурном режиме | Дистанционное управление (500 м на $f$ = 140...170 МГц). Кварцевая стабилизация частоты |

Окончание табл. 1.3.1

| Вид исполнения | Индекс | Частота, МГц<br>Вид модуляции | Вых. мощн., мВт<br>Дальн. действия, м | Габариты, мм<br>Масса, г | Тип антенны<br>Питание, В | Время работы, ч | Примечание |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Авторучка | «Авторучка» | 300<br>*Широкополосная* частотная | ——<br>100 | 135×10,5 | Встроенная<br>2 элемента V 393 | 6 | Кварцевая стабилизация частоты |
| Наручные часы | РК1025-SS | 427<br>Узкополосная частотная | | ф 25×4<br>40 | ——<br>1,5 | 6 | Кварцевая стабилизация частоты. Встроенный переключатель *«вкл/выкл.»* |
| Кожаный ремень | МКС-1392 | 427<br>Широкополосная частотная | 300<br>1÷6×10$^3$ | ——<br>300 | ——<br>8×1,5 | 8 | Кварцевая стабилизация частоты |
| Зажигалка | Cricket | 447...459<br>Широкополосная частотная | ——<br>100 | 77×22×13 | Спиральная<br>2×1,5 | 25 | Дальность перехвата разговора 10 м |
| Калькулятор | «Калькулятор-475» | 470...475<br>Широкополосная частотная | ——<br>50 | 140×9 | Внутренняя<br>3,2 | 48 | Схемотехническая стабилизация частоты |
| Пачка сигар | «РМ-пачка сигар» | 630...640<br>Частотная | 1 | | ——<br>3 | 50 | |

**Таблица 1.3.2. Основные характеристики полуактивных акустических радиозакладок**

Характеристики /SIM-ATP-16 /SIM-ATP-40

Фирма-производитель /Hildenbrand-Elektronik GmbH /Hildenbrand-Elektronik GimbH
Вид исполнения /Обычный
Частота облучающего сигнала, МГц /160 /800...950
Частота переизлученного сигнала, МГц /160,012 /800...950
Вид модуляции /Узкополосная частотная
Мощность передатчика облучающего сигнала /10 Вт /100 мкВт...20 мВт (мощность облучающего сигнала)
Размеры, мм /90x90x4 /130x75x250
Питание, В / /3
Время работы /2000...4000 ч /4 месяца
Примечание /В исходном состоянии упакован в фольгу. Время хранения 2 года. Всенаправленная кольцевая антенна. Частотный диапазон звукового сигнала 75...10 000 Гц /Время хранения в стандартной упаковке 10 лет. Направленная директорная антенна. Частотный диапазон звукового сигнала 75...10 000 Гц Потери при преобразовании - 8 дБ

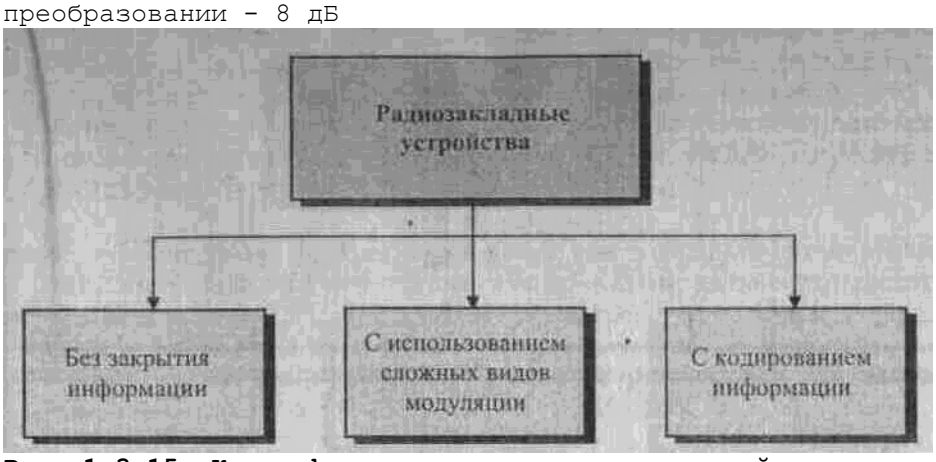



**Рис. 1.3.15. Классификация радиозакладных устройств по способу закрытия информации**

Естественно, что наиболее простым видом ЗУ являются радиозакладки без закрытия информации. Однако их применение ограничено возможностью перехвата информации любым лицом, имеющим приемник, работающий на частоте РЗУ.

К радиозакладкам с использованием сложных видов модуляции относятся устройства с двойной модуляцией сигнала — на поднесущей и основной частоте излучения, например, РК1970-SS (табл. 1.3.1). Частота поднесущей выбирается много больше 20 кГц. Поэтому прием информации возможен только на специальный приемник с двойным детектированием, что существенно повышает ее скрытность. Попытка прослушивания сигнала обычным приемником ни к чему не приведет, так как выходной сигнал будет превышать верхний частотный уровень чувствительности человеческого уха.

К более эффективным способам закрытия информации относится использование сложных шумоподобных сигналов и различных способов кодирования информации.

Так например, шумоподобные сигналы с фазовой манипуляцией используются в радиозакладках **РК1970 и SIM-PR-9000T**, а аналоговое скремблирование (наиболее часто применяемый способ шифрования) — в радиозакладках **РК2010S** (простая инверсия спектра) и в устройствах **«Брусок-ЛЗБ ДУ»**, **РК1380-SS** или **РК540-SS** (сложная инверсия спектра).

Более сложный способ шифрования речевой информации — кодирование ее в цифровом виде. Такой способ закрытия применен, например, в радиозакладках **РК1195-SS**, РК2050, **SIM-PR-9000T и РК1970 (см.** табл. 1.3.1).

В зависимости от мощности передатчика РЗУ делятся на три вида — малой, средней и большой дальности действия (рис. 1.3.16).

Радиозакладные устройства малой дальности способны передавать информацию на расстояние, не превышающее несколько десятков метров,

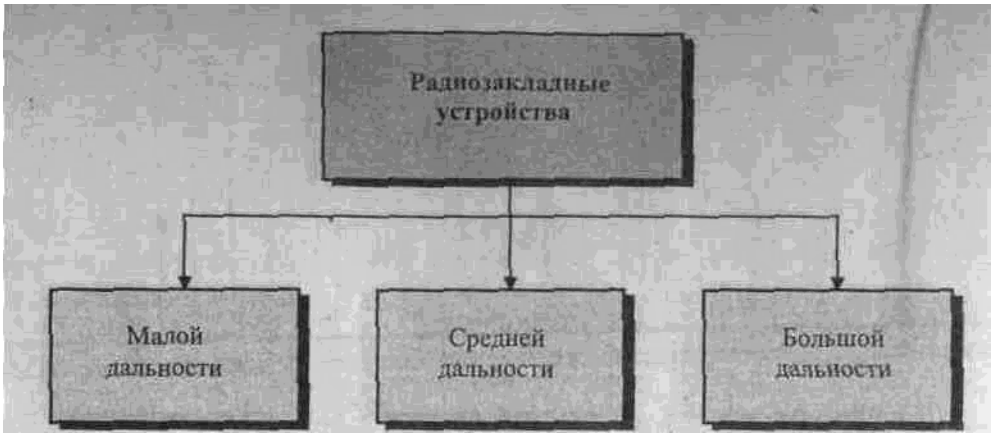



**Рис. 1.3.16. Классификация радиозакладных устройств по дальности действия**

поэтому без ретранслятора (приемно-передающего блока) они, как правило, не используются. РЗУ средней дальности позволяют вести уверенный прием информации на удалении несколько сот метров, а радиозакладки большой дальности способны работать с радиоприемными устройствами, расположенными на удалении 1000 м и более.

В качестве иллюстрации можно привести характеристики некоторых типов серийно выпускаемых закладных устройств:

РК580-S — передатчик с кварцевой стабилизацией частоты, закамуфлированный под поясной ремень. Вес — 250 г. Мощность излучения — 50 мВт, рабочая частота — 139 МГц, дальность передачи радиосигнала — 700 м. Источник питания — батарея с напряжением 6 В. Рекомендуемые приемники для работы с данным радиомикрофоном: **РК830-SS, РК1015-SS.**

**РК525-S** — передатчик с кварцевой стабилизацией частоты, закамуфлированный в головном уборе. Вес — 150 г. Рабочая частота —139 МГц. Источник питания — батарея с напряжением 6В.

**РК585-S** — передатчик с кварцевой стабилизацией частоты, закамуфлированный под авторучку диаметром 11 мм и длиной 135 мм. Вес — 30 г. Рабочая частота — 139 МГц. Дальность перехвата акустических сигналов — 5м, дальность передачи радиосигналов — 300 м. Источник питания — 2 батареи с напряжением по 1,5 В. Рекомендуемые приемники для работы с данным радиомикрофоном: **РК830-SS, РК825-S, РК1015-SS.**

**РК575-S —** передатчик с кварцевой стабилизацией частоты, закамуфлированный под зажигалку диаметром 55 мм и длиной 73 мм. Вес — 95 г. Источник питания — батарея с напряжением 6 В. Рекомендуемые приемники для работы с данным радиомикрофоном: **РК830-SS, РК815-S, РК1015-SS.**

**РК560-S** — передатчик, закамуфлированный под электролампочку. Дальность перехвата акустических сигналов — 20 м, дальность передачи радиосигналов — 300 м. Питается от электросети переменного тока с напряжением 110/220 В. Не может быть использован в качестве источника света. Рекомендуемые приемники для работы с данным радиомикрофоном: **РК830-SS, РК825-S, РК1015-SS.**

**РК570-S** — передатчик, закамуфлированный под пепельницу. Габариты — 125х12х30 мм, вес — 275 г. Дальность передачи радиосигналов — 250 м. Источник питания — батарея с напряжением 9 В, время непрерывной работы — 50 часов. Дистанционное управление режимом излучения.

**РК1025-S** — передатчик, закамуфлированный под наручные часы. Представляет из себя диск диаметром 25 мм и толщиной 4 мм, вес 40 г. Питается от одного элемента 1,5 В, которого хватает на 6 часов непрерывной работы. Частоты излучений лежат в диапазонах 88...108;

130...150 МГц. Рекомендуемый приемник для работы с данным радиомикрофоном: **РК1015-SS.**

**STG 4005** — радиомикрофон с акустоматом, работает в диапазоне частот 130...150 МГц, вид модуляции — широкополосная частотная, выходная мощность — 6 мВт. Габариты — 45х30х15 мм, вес — 35 г, напряжение питания — 6В, тип антенны — гибкая.

**STG 4007** — радиомикрофон с акустоматом, работает в диапазоне частот 395...415 МГц, вид модуляции — узкополосная частотная, выходная мощность — 15 мВт. Габариты — 66х27х14 мм, вес — 52 г, напряжение питания — 6В, тип антенны — гибкая.

**GTG 4215** — радиомикрофон с дистанционным управлением, работает в * диапазоне частот 115... 150 МГц, вид модуляции — широкополосная частотная, выходная мощность — 5 мВт. Габариты — 67х36х25 мм, вес — 70 г, напряжение питания — 110/220 В электросети переменного тока, антенна — провод электросети.
Устройство дистанционного управления работает в диапазоне частот:
800...1000 Гц. Выходная мощность — 50 мВт, команда — кодированная. Габариты — 155х60х20 мм, вес — 70 г.
**UXMC** — радиомикрофон, закамуфлированный в виде портативного компьютера с сетевым или батарейным электропитанием. Может использоваться и как обычный компьютер, и как радиомикрофон для передачи перехватываемых речевых сигналов из контролируемого помещения на расстояние до 3000 м. Диапазон рабочих частот — 398...430 МГц с выделением шести фиксированных частот.
Устройство поставляется в комплекте с миниатюрным приемником, оборудованным шумоподавителем и имеющим возможность подключения диктофона с длительностью записи 1,3 или 6 часов.
**UX CARD** — радиомикрофон, закамуфлированный в виде кредитной карточки. Работает в диапазоне частот 398...430 МГц. Имеет размеры кредитной карточки толщиной 4 мм. Он может быть скрыт между страницами книги, вставлен в один из настольных канцелярских приборов, размещен в кармане одежды или сумке. Время непрерывной работы прибора — 30 часов, дальность передачи — 200...300 м. Электропитание от встроенной литиевой батареи с напряжением 3 В.
**UXP** — радиомикрофон, закамуфлированный в корпус шариковой ручки типа Parker. При этом остается место для миниатюрного пишущего стержня. Дальность действия до 300 м. Ручку с встроенным устройством можно держать в кармане или пользоваться ею открыто, не вызывая подозрений у окружающих. Электропитание от двух элементов с напряжением 1,5 В, размещенных в корпусе авторучки.
**UXC** — радиомикрофон, закамуфлированный в виде карманного калькулятора. Работает в диапазоне частот 398...430 МГц, дальность передачи информации 300—1000 м. Устройство наделено всеми функциями обычного калькулятора, поэтому может быть размещено в непосредственной близости от прослушиваемого источника речевой информации.
Фирма SIM Security and Electronic Systems (Германия) предлагает серию радиомикрофонов. Ниже дается краткое описание некоторых изделий.
**Одноплатные радиомикрофоны серии Model SIM-A-40** предназначены для встраивания в различные офисные и бытовые предметы без изменения их конструкции или внешнего вида.
Все радиомикрофоны указанной серии изготовлены по технологии поверхностного монтажа. Исключительно плоская форма им придается благодаря покрытию схемной платы специальным полимером. Поэтому их можно встраивать так, что затем трудно обнаружить даже при тщательном внешнем осмотре. Важным элементом каждого радиомикрофона является высокочувствительный акустический датчик.
Кроме входящих в серию **SIM-A-40** встраиваемых радиомикрофонов в нее входит также радиомикрофон **SIM-A-45GS**, маскируемый в поясном ремне. Выходная мощность этого радиомикрофона равна 10 мВт. По желанию заказчиков его мощность может быть повышена до 30 мВт. Сигналы радиомикрофонов могут приниматься обычными радиоприемниками и сканерами.

**Технические характеристики микрофонов A-40EB, A-41-SM, A-42TR**

Модель /A-40EB /A-41-SM /A-42TR
Камуфляж /Радиоэлектронный прибор /Портфель /Авторучка
Диапазон частот, МГц /130-180 /130-180 /130-180
Выходная мощность, мВт /5 /60 /20
Модуляция /Узкополосная ЧМ /Узкополосная ЧМ /Узкополосная ЧМ
Ширина полосы звуковых частот, кГц /10 /10 /10
Электропитание /Кадмиевая аккумуляторная батарея, четыре элемента
Потребляемый ток, мА /— /— /25

**Технические характеристики микрофонов A-43FH, A-44VT, A-45GS**

Модель /A-43FN /A-44VT /A-45GS
Камуфляж /Авторучка /Включаемый /Поясной ремень

Диапазон частот, МГц /130-180 /130-180 /130-180

Выходная мощность, мВт /20 /6 /10/30

Модуляция /Узкополосная ЧМ /Узкополосная ЧМ /Узкополосная ЧМ

Ширина полосы звуковых частот, кГц /10 /10 /10

Электропитание /Два кнопочных элемента 2x1 Вт /Электросеть 220 В, 50 Гц /Источник пост. тока 2,4—4,5 В

Потребляемый ток, мА /25 /10 /12 при 2,4 В 22 при 4,5 В

**Радиомикрофоны Model** SIM-A-46/47 предназначены для маскировки их в престижных авторучках или карманных калькуляторах. Для скрытых операций выпускаются также миниатюрные радиоприемники, настроенные на заданные радиочастоты (с кварцевой стабилизацией). Каждый радиомикрофон имеет высокочувствительный микрофон и источник электропитания. Передатчик радиомикрофона может находиться в дежурном режиме 2000 ч без смены источника питания. Продолжительность непрерывной работы в режиме передачи — 3 ч.

**Технические характеристики**

Модель /SIM-A-46 /SIM-A-47

Камуфляж /Авторучка /Калькулятор

Диапазон частот, МГц /350-400 /350-400

Выходная мощность, мВт /1/1

Частота сигнала бедствия, Гц /2 (включено/выключено) /2 (включено/выключено)

Шумоподавление, дБ /30 /30

Продолжительность работы в дежурном режиме, ч /2000 /2000 .

Электропитание /Три элемента типа У13А или 393 /Два элемента типа СК2016 или 1 элемент 675РХ

**Сверхминиатюрный радиомикрофон Model SIM-A-64** встраивается в телефонные розетки и аппараты. Он предназначен для прямой радиопередачи телефонных разговоров.

Радиомикрофон изготовлен по технологии поверхностного монтажа. Его схемная плата покрыта специальным полимером. Она имеет форму очень тонкой пластинки, которая может закладываться в телефонные аппараты, интерфейсы или в телефонные линии. Электропитание радиомикрофона осуществляется от телефонной сети. Вследствие очень небольшого потребления тока и малого последовательного сопротивления радиомикрофойа его подключение к телефонной линии практически не нарушает ее нормальной работы.

Сигналы радиомикрофона могут приниматься обычными или сканирующими радиоприемниками.

**Технические характеристики**

Диапазон радиочастот, МГц... 130—180 (с кварцевой стабилизацией)
Модуляция..... узкополосная, частотная
Ширина полосы звуковых частот, кГц.... 7
Электропитание ..... от телефонной линии,
напряжение не менее 1,5 В Размеры, мм..... 8x6x20

**Одноплатный радиомикрофон Model-SIM-65** может работать в диапазонах ОВЧ или УВЧ (с кварцевой стабилизацией частоты). Выходная мощность версии ОВЧ может переключаться от 10 до 300 мВт, а версия УВЧ постоянна и равна 50 мВт.

Радиомикрофон представляет собой одну схемную микроплату, изготовленную по технологии с поверхностным монтажом. На плате расположен также высокочувствительный электретный микрофон. Плата покрыта специальным полимером, защищающим электронные компоненты. Она имеет форму плоской монолитной пластинки, толщина которой не превышает 6 мм. Электропитание возможно от встроенной батареи или от внешнего источника напряжением 9 В. Прием сигналов радиомикрофона может осуществляться обычными или сканирующими радиоприемниками.

По отдельному заказу может поставляться радиомикрофон этой модели, скрытый в поясном ремне и рассчитанный на прием сигналов бедствия.

**Технические характеристики**

Диапазон /ОВЧ /УВЧ

Диапазон рабочих частот, МГц. /140-180 /400-450

Выходная мощность, мВт /30/300 /50

Модуляция /Узкополосная. частотная /Узкополосная частотная

Электропитание, В /9 /9

Потребляемый ток, мА /70 /50

Размеры, мм /20x4x45 /20x4x45

**Радиомнкрофон Model** SIM-A-75 разрабатывался фирмой при непосредственном участии заказчика для выбора конструкции, наиболее соответствующей его требованиям. В качестве примеров возможного конструктивного оформления камуфляжа радиомикрофона SIM-A-75 приводятся следующие:

>- в портфеле типа «дипломат» со свободным выбором модели радиомикрофона, набором определенных функций управления, встроенным блоком электропитания;

>- в портативном блоке электропитания с ручным и дистанционным управлением радиомикрофоном, с кодированием и без кодирования передаваемых сигналов и нормальным использованием блока электропитания по его назначению;

>- в форме брелка для ключей, с переключателем для передачи сигнала тревоги и встроенным источником питания.

В таких вариантах оформления максимально учитываются требования заказчиков. Могут быть разработаны новые варианты.

**Радиомикрофоны Model SIM SAW-1X, SIM SAW-10X, SIM SAW-13, -15, -16, -19 и SIM SAW-103, -105, -108, -109** обеспечивают высококачественную передачу звуковой информации в широком диапазоне радиочастот. Возможность использования для их электропитания различных источников (батареи сухих элементов, аккумуляторные батареи, внешние источники) допускает их применение как в качестве носимых под одеждой, так и стационарных приборов. Радиомикрофоны этих моделей имеют встроенный и поставляемый по отдельному заказу высокочувствительный микрофон. Задающий генератор передатчика с резонатором на поверхностных акустических волнах (SAW) генерирует спектрально чистые, свободные от субгармоник колебания. Предварительная обработка входных сигналов звуковых частот включает их плавное ограничение и сжатие.

Радиомикрофоны могут непрерывно работать с электропитанием от батарей сухих элементов напряжением 2—3 В в течение 8 ч, а от аккумуляторной батареи напряжением 2—3 В до 4 ч.

**Технические характеристики**

Диапазон радиочастот, МГц

Model-13/-103 ..... 293—325

Model-14/-104..... 403—447

Model-16/-106..... 640—680

Model-19/-109..... 905—917

Задающий генератор..... с резонатором на поверхностных акустических волнах

Качество передаваемых радиосигналов.... высокая спектральная чистота, отсутствие субгармоник

Выходная мощность на радиочастотах

Model-lX ..... 1 мВт, 3В на сопротивлении

500м Model-l0X ..... 10 мВт, 3В на сопротивлении

500м Модуляция..... широкополосная, частотная

Ширина полосы звуковых частот, Гц..... 100—7000

Обработка сигналов звуковых частот .... плавное ограничение (в широком динамическом диапазоне)

Микрофоны ..... встроенный или внешний с дальностью действия до 1 м

Электропитание ..... внешний источник постоянного тока,3В

Защита электропитания..... от перемены полярности, стабилизация тока;

Диапазон рабочих температур, °С ..... от 0 до +60

Размеры, мм..... 29x7x4

**Радиомикрофоиы Model SIM-SAW-50X, SIM-SAW-503, -505, -506, -509**

отличаются высококачественной передачей звуковой информации. Они имеют или встроенный, или внешний микрофон. Возможность работы от различных источников электропитания (батарея сухих элементов, аккумуляторная батарея, внешний источник) расширяет их применение (скрытое ношение в одежде, фиксированные закладки).

**Технические характеристики**

Диапазон радиочастот, МГц

Model-503 .....293—325

Model-504 ..... 403—447
Model-506..... 640—680
Model-509 ..... 905—917
Задающий генератор..... с резонатором на поверхностных акустических волнах
Качество передаваемых радиосигналов..... высокая спектральная чистота, отсутствие субгармоник
Выходная мощность на радиочастотах
(все модели) ..... 50 мВт, 3В на сопротивлении
500м Модуляция..... широкополосная, частотная
Ширина полосы звуковых частот, Гц..... 100—7000
Обработка сигналов звуковых частот ..... плавное ограничение (в широком динамическом диапазоне)
Микрофоны ..... встроенный или внешний с дальностью действия до 1м
Электропитание..... внешний источник постоянного тока,3В
Защита электропитания..... от перемены полярности, стабилизация тока
Диапазон рабочих температур, °С ..... от 0 до -60
Размеры, мм..... 29x7x4

**Радиомикрофон SIM-A-99** рассчитан на скрытое применение в качестве прибора личной самозащиты и передатчика сигналов бедствия. Он передает сигнал тревоги в виде ультразвуковых импульсов длительностью 250 мс в течение 30 с. Прием этого сигнала указывает на то, что радиомикрофон находится в пределах дальности действия радиоприемника. Такой сигнал более защищен от перехвата, чем непрерывный сигнал. Кроме передачи сигналов бедствия, радиомикрофон может действовать как передатчик звуковых сигналов тревоги.

SIM-A-99 выпускается с четырьмя диапазонами рабочих частот: 150—180 МГц, 210—220 МГц, 380—420 МГц, 800—930 МГц. При включении радиомикрофона в режим передачи сигналов тревоги он излучает импульсные сигналы длительностью 250 мс в течение 30 с при выходной мощности 1 Вт. Никто, кроме владельца радиомикрофона, не может обнаружить включение сигнала тревоги.

**Технические характеристики**

Модуляция..... узкополосная, частотная
Ширина полосы звуковых частот, Гц..... 100—7000
Частотный интервал между каналами с ЧМ (в диапазоне радиочастот до 420 МГц), кГц ... 25
Электропитание ..... от внешних источников постоянного тока Диапазон рабочих температур, °С ..... от -20 до +60
Размеры, мм..... 32x6x32

**Радиомикрофоны SIM-PLL-10X, SIM-PLL-100X.** В радиомикрофонах указанных моделей применены: цепь фазовой автоподстройки частоты PP1 (Phase Lock Loop), плавное ограничение и сжатие сигналов звуковых частот и автоматическая регулировка усиления. Передатчики радиомикрофонов этих моделей отличаются по выходной мощности и диапазонам радиочастот. Выпускаются модели с диапазонами частот: 150—180 МГц, 210—220 МГц, 380—420 МГц, 800—930 МГц.

Кроме встроенного микрофона может применяться внешний микрофон. Для электропитания используются внешние источники постоянного тока. Прием сигналов радиомикрофонов производится специальными радиоприемниками.

**Технические характеристики**

Выходная мощность на радиочастотах, мВт ... 10 (PLL-10X) или 100(PLL-100X)
Модуляция..... узкополосная, частотная
Ширина полосы звуковых частот, Гц..... 100—7000
Частотный интервал между каналами с ЧМ
(в диапазоне частот до 420 МГц), кГц .. 25
Электропитание..... внешний источник постоянного тока, 3 В
Диапазон рабочих температур, °С ..... от -20 до +60
Размеры, мм..... 32x6x32

**Миниатюрные радиомикрофоны Model SIM-TX-928, SIM-TX-928A** имеют плоскую форму и отличаются высокой выходной мощностью на радиочастотах в диапазоне ОВЧ 150—174 МГц. Они имеют входы для подключения внешних микрофона, источника электропитания и антенны.

Model SIM-TX-928A имеет скремблер. Для электропитания радиомикрофонов используются внешние источники постоянного тока (батарея сухих элементов или аккумуляторная батарея) напряжением 9 В.
Прием сигналов радиомаяков возможен на обычные и сканирующие радиоприемники.

**Технические характеристики**

Диапазон радиочастот, МГц..... 150—174
Выходная мощность, мВт..... 1000
Скремблирование..... Model TX-928A
Стабильность частоты..... $\pm 10^{-6}$
Микрофон..... внешний электретный
Электропитание ..... внешний источник питания
(батарея), 9
В Размеры, мм..... 80x55x9,5
Масса, г..... 79

**Радиомикрофоны Model SIM-TX-915, SIM-TX-916** рассчитаны на ношение под одеждой. Они имеют форму прямоугольной пластины толщиной не более 20 мм, оснащены гнездами и зажимами для подключения внешних микрофона, источников электропитания и проволочной антенны.
Диапазон частот радиомикрофонов TX-915 и TX-916 находится в пределах от 150 до 174 МГц. Выходная мощность на этих частотах постоянна и равна 1000 мВт.
Радиомикрофон TX-916 отличается наличием скремблера сигналов. Для электропитания необходимы две батареи сухих элементов или аккумуляторная батарея напряжением 9 В. Продолжительность непрерывной работы от этих источников составляет 3 ч.
Прием сигналов от радиомикрофонов возможен всеми обычными и сканирующими радиоприемниками с соответствующим диапазоном частот.

**Технические характеристики**

Модель ..... SIM-TX-915, SIM-TX-916
Диапазон частот, МГц ..... 150—174
Выходная мощность, мВт..... 1000
Стабильность частоты..... $\pm 10^{-6}$
Микрофон..... внешний
Электропитание..... внешний источник постоянного тока,9 В
Продолжительность непрерывной работы, ч..... 3
Размеры, мм..... 87x57x19
Масса, г ..... 184

**Миниатюрный радиомикрофон SIM-A31** передает аудиоинформацию от внешнего или встроенного микрофона или из телефонной линии (по отдельному заказу) на радиочастотах диапазона ГГц.
Внешний микрофон соединяется с передатчиком коаксиальным кабелем. Уровень входного сигнала — 20 дБ на сопротивлении 600 Ом. Радиомикрофон имеет антенну с усилением 6 дБ. Внешний шум эффективно подавляется экспандером, что повышает качество передаваемых сигналов звуковых частот.

**Технические характеристики**

Рабочая частота, ГГц ..... 10,5
Выходная мощность, мВт..... 30
Модуляция..... широкополосная, частотная F-3-W
Электропитание ..... источник постоянного тока, 8—14 В (с защитой от перемены полярности Потребляемый ток, мА..... 40
Диапазон рабочих температур, °С ..... от - 10 до +50
Размеры, мм..... 40x27x13
Масса, г..... 25
Уровень входного сигнала
звуковой частоты, дБ..... -20 на сопротивление 6000м

Для приема сигналов радиомикрофона придается специальный радиоприемник с антенной (усиление 30 дБ).
Фирма M.A.I.M.S. (США) предлагает специальную технику, краткое описание которой представлено ниже.
**Радиопередатчик SRG 4100-PENTX-U**, замаскированный в авторучке, имеет встроенные антенну и сверхвысокочувствительный микрофон. Применена кварцевая стабилизация

частоты.

**Технические характеристики**

Длина, мм..... 130
Масса, г ..... 20
Электропитание, В..... батарея из двух элементов SR-48W напряжением 1,55В
Продолжительность непрерывной работы от батареи, ч ..... около 15
Дальность передачи, м ..... до 200

**Носимый под одеждой радиопередатчик STG 4002-QTX-U** с кварцевой стабилизацией частоты предназначен для скрытой передачи аудиоинформации. Передатчик имеет гибкую штыревую антенну, которая легко скрывается под одеждой.

**Технические характеристики**

Размеры, мм..... 66x27x144
Масса, г ..... 70 с батареей
Электропитание ..... один литиевый элемент СК-2Т (1,5 В) или два сухих элемента (3В);
Продолжительность непрерывной работы от батареи, ч ..... 130
Дальность передачи, м ..... до 1000

Внешний вид некоторых радиозакладных устройств в обычном и закамуфлированном исполнении показан на рис. 1.3.17, а схемы применения — на рис. 1.3.18.

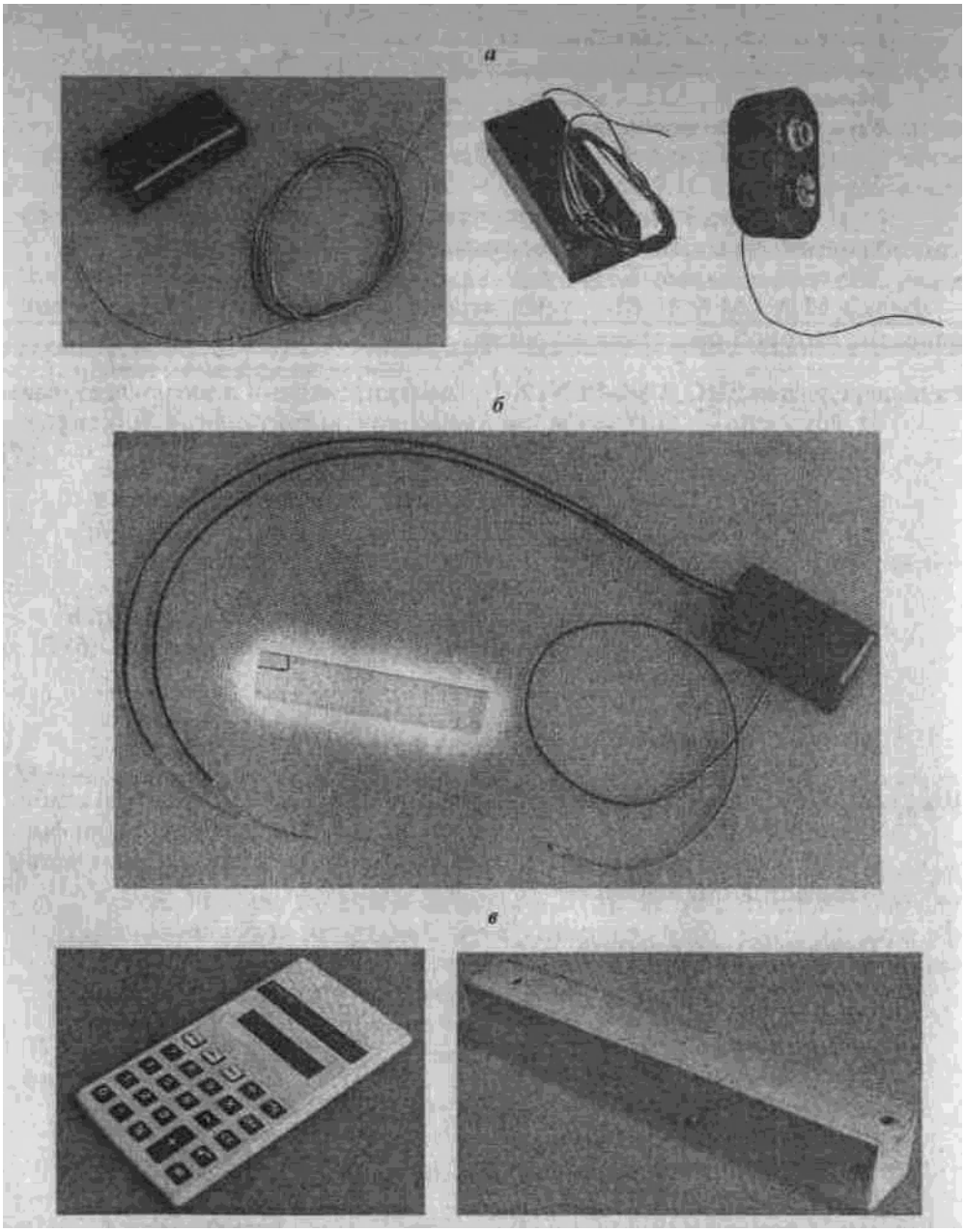
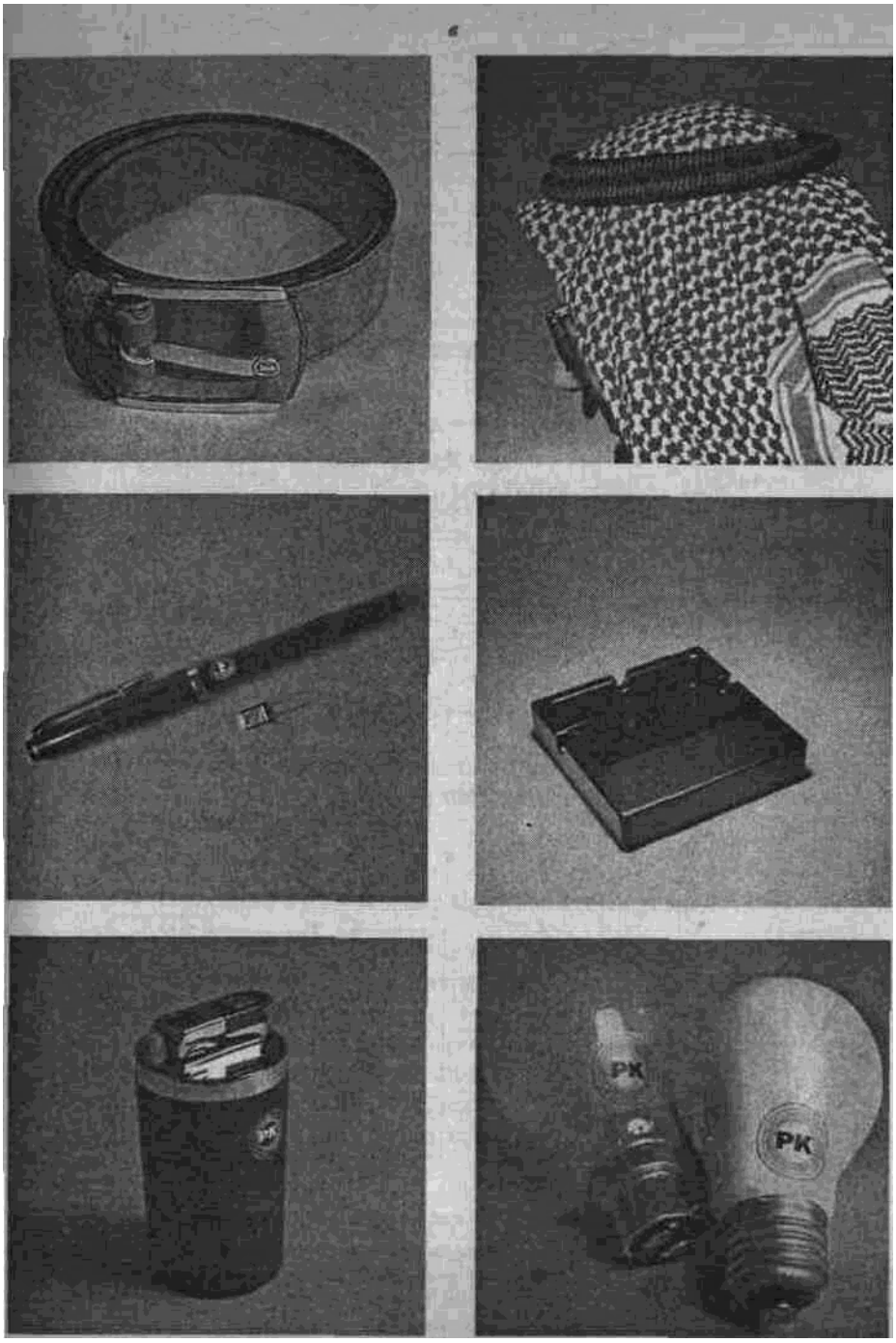



**Рис. 1.3.17. Радиозакладные устройства:**
а — радиомикрофоны в обычном исполнении; б — радиозакладное устройство в обычном исполнении, предназначенное для подключения к телефонным линиям связи; в — радиомикрофоны в закамуфлированном виде


PK
PK
PK

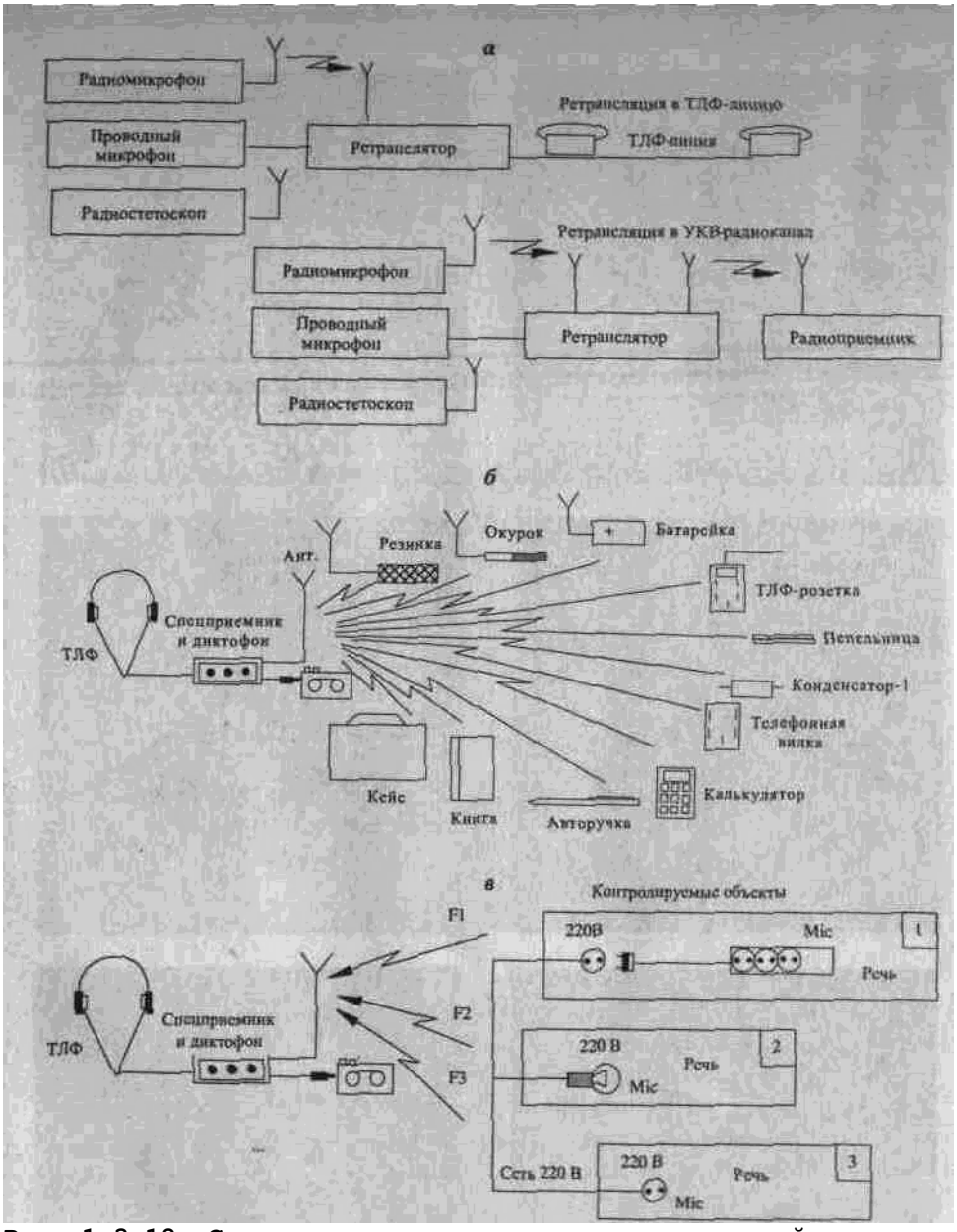



**Рис. 1.3.18. Схемы применения радиозакладных устройств:**
а — с использованием ретрансляторов сигналов от закладных устройств к пунктам приема и сбора информации; б — на один приемник от нескольких закамуфлированных под личные вещи закладных устройств; в — на один приемник от нескольких закамуфлированных под элементы электроцепей радиозакладных устройств

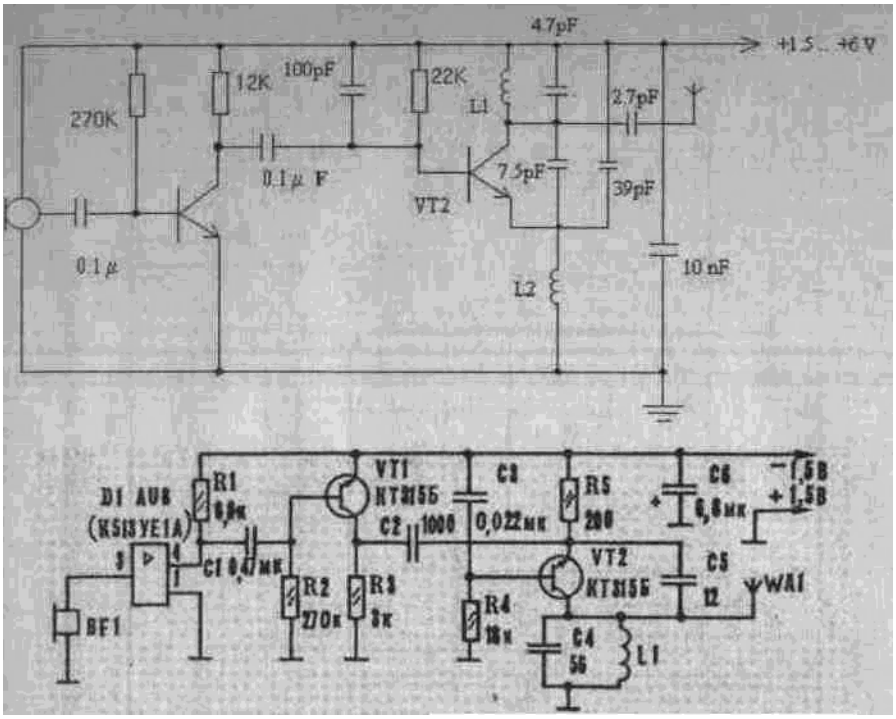



**Рис. 1.3.19. Простейшие примеры построения радиомикрофонов**

Для того чтобы дать представление о принципах построения закладных устройств, на рис. 1.3.19, 1.3.20 приведены несколько вариантов принципиальных схем радиомикрофонов.

**Приемники излучения радиозакладных устройств**

Для приема информации, передаваемой с радиозакладок, могут быть использованы различные виды радиоприемных устройств. Наиболее часто для этих целей используют:

>- портативные сканерные приемники;

**>-** специальные приемные устройства;

>- приемники портативных радиостанций;

>- бытовые радиоприемники.

Современные переносные малогабаритные (портативные) сканерные приемники имеют автономные аккумуляторные источники питания, свободно умещаются во внутреннем кармане пиджака, а их вес составляет 150...350 г.

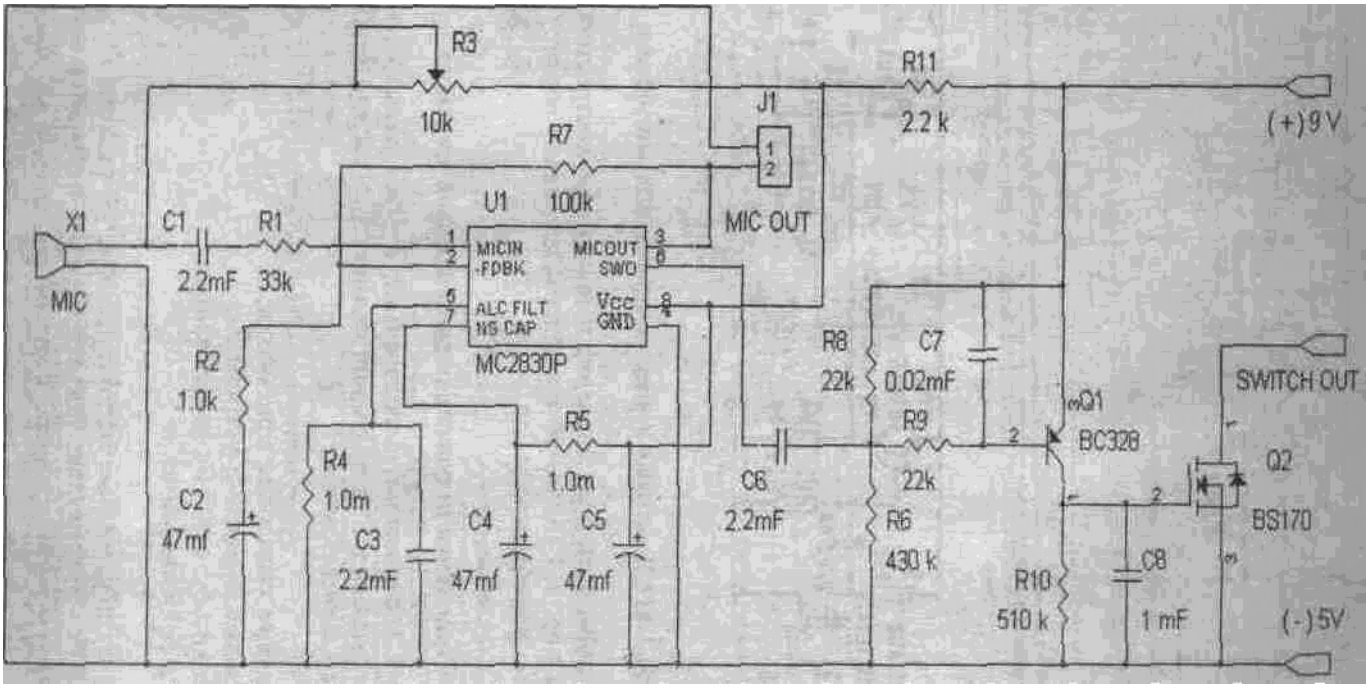



**Рис. 1.3.20. Принципиальные схемы построения высококачественных радиомикрофонов**

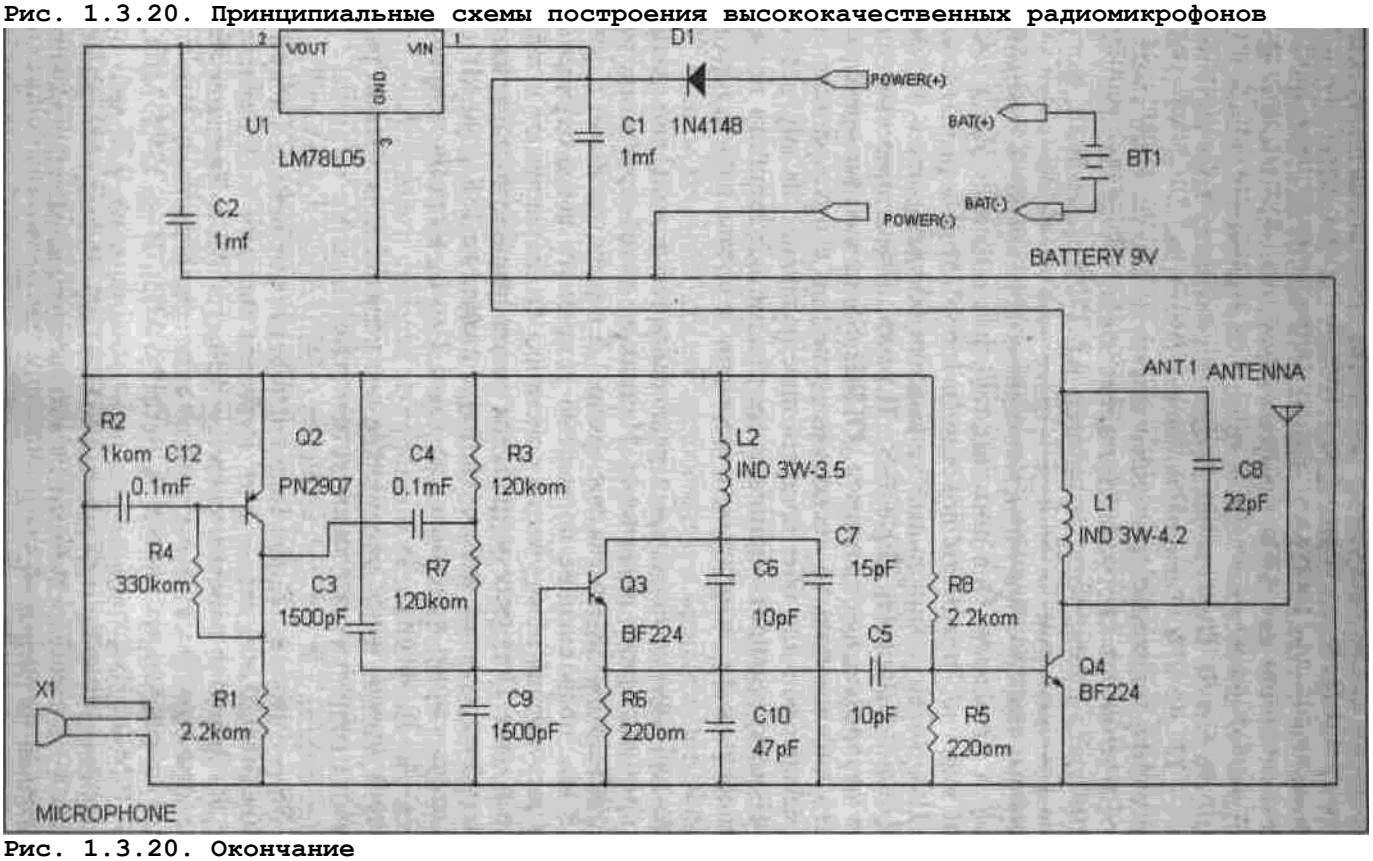



**Рис. 1.3.20. Окончание**

Несмотря на малые габариты и вес такие приемники позволяют осуществлять прием сигналов в диапазоне 100 кГц ...1300 МГц, а некоторые типы приемников — до 1900 МГц и даже до 2060 МГц («HSC-050»). Они обеспечивают прием сигналов с амплитудной, узкополосной и широкополосной частотной модуляцией, а их чувствительность лежит в пределах от 0,35 до 6 мкВ. Полоса пропускания в режиме приема узкополосных сигналов — 12... 15 кГц, а широкополосных (текстовых) — 150... 180 кГц.

Портативные сканерные приемники имеют от 100 до 1000 каналов памяти и обеспечивают скорость сканирования до 30 каналов в секунду. Некоторые типы приемников, например

**AP-2700 и AR-8000**, могут управляться компьютером.
Для приема информации от радиозакладок используют и специальные приемные устройства. Они выпускаются как в обычном, так и камуфлированном виде под предметы повседневного обихода или бытовые приемники. Некоторые специальные приемники оборудованы встроенными магнитофонами (например, PK820-S). В ряде случаев применяются специальные комплексы, как, например, **PK1015-SS**, способные одновременно принимать информацию по нескольким каналам и осуществлять ее запись на магнитофон или обеспечивать прослушивание на внутренние динамики. Чувствительность специальных приемных устройств не уступает чувствительности сканерных приемников и составляет величину менее 0,5 мкВ.
Иногда для приема сигналов с радиозакладок используют специальные сверхминиатюрные приемники. Например, такой приемник, работающий в УКВ-диапазоне, имеет вес около 1,5 г (с батарейкой) и размеры 17,5x11,5 мм, позволяющие полностью установить его в слуховой проход. Для затруднения обнаружения приемника его окрашивают в телесный или темный цвет. Приемное устройство имеет кварцевую стабилизацию и может быть настроено на любую частоту в диапазоне 138... 190 МГц. Чувствительность такого приемника не хуже 2 мкВ, а время непрерывной работы — 15... 30 часов.
Примером специальных приемников для перехвата излучений радиозакладок могут служить следующие устройства:
**PK1015-SS** — приемник, размещенный в атташе-кейсе. Габариты — 460x330x120 мм, вес — 5 кг. Источник питания — 8 элементов по 1,5 В. Диапазон рабочих частот — 130...150 МГц. Значение рабочей частоты выводится на жидкокристаллический дисплей. Имеет 3 канала кварцованных частот: А — 139,6 МГц, В — 139,8 МГц, С — 140,0 МГц. Чувствительность приемника не хуже 0,25 мкВ при отношении сигнал/шум на выходе РПУ 12 дБ. Время непрерывной работы — 2 часа. Предусмотрена автоматическая запись принимаемых сигналов на диктофон.
**PK830-SS** — приемник с габаритами, позволяющими размещать его в стандартной пачке сигарет: 85x54x20 мм, вес — 275 г. Источник питания — элемент с напряжением 9 В. Диапазон рабочих частот — 120...150 МГц. Имеет 3 канала кварцованных частот: А — 139,6 МГц, В — 139,8 МГц, С — 140,0 МГц. Чувствительность приемника не хуже 0,25 мкВ при отношении сигнал/шум на выходе РПУ 12 дБ.
**UXR1** — двухканальный радиоприемник, работающий в диапазоне частот 398...430 МГц. Может одновременно принимать передачи от двух радиомикрофонов с попеременным переключением каналов. Габариты — 48x66x19 мм, электропитание — литиевая батарея напряжением 6 В, время непрерывной работы — 36—48 часов. Дальность приема сигналов — 150—1000 м.
**UXR3** — высокочувствительный двухканальный радиоприемник диапазона частот 398-430 МГц, объединенный с аудиомагнитофоном. Предназначен для установки в транспортные средства. Электропитание — 12В, дальность приема — до 2000 м.
**UXR5** — четырехканальный радиоприемник — аудиомагнитофон, размещенный в портфеле типа «дипломат». Рабочий диапазон — УВЧ. Оснащен автоматическим управлением и миниатюрным компьютером для опознавания голосов, перехватываемых радиомикрофонами в контролируемых помещениях. В блок входит аудиомагнитофон с автоматическим реверсом, рассчитанный на непрерывную запись в течение 2 часов.
**Двухканальный радиоприемник STG 4401-RX-P2-U** — легкий компактный и портативный радиоприемник с двумя переключаемыми каналами дает возможность держать связь с двумя радиопередатчиками. Приемник имеет выходы на головной телефон и магнитофон, что позволяет использовать его одновременно для радиоконтроля и регистрации принимаемых сообщений. Светодиодный индикатор со штриховой индикацией сигнализирует о работающих передатчиках и позволяет определять уровень принимаемых сигналов. Приемник имеет штыревую антенну и, кроме того, может подключаться к комплекту настроенных антенн **STG 1720-A** с магнитным креплением, устанавливаемым на крыше кузова автомобиля радиоконтроля. В комплект **STG** 1720-А входят спиральная и штыревая антенны и соединительный провод длинной 2 м. Антенны комплекта могут использоваться с радиоприемником отдельно в качестве портативного прибора.
**Технические характеристики**
Размеры, мм..... 112,5x80x30
Масса, г ..... 300 с батареей
Электропитание ..... батарея М 1604,9В

Продолжительность непрерывной работы от батареи, ч ..... 20
Внешний вид некоторых приемных устройств приведен на рис. 1.3.21
Для приема излучений радиозакладок, работающих в диапазоне 134... 174 МГц, 400...512 МГц могут использоваться портативные радиостанции. Они имеют высокую чувствительность (0,25...0,5 мкВ) и малые габариты.
Основным достоинством применения таких приемников является возможность приема кодированных сигналов, так как современные радиостанции оборудуются встроенными скремблерами. Недостатком является то, что портативные радиостанции обеспечивают высокое качество приема сигналов только от радиозакладок, имеющих узкополосную частотную модуляцию и использующих кварцевую стабилизацию частоты.
Для приема информации, передаваемой с радиозакладок, которые работают в диапазоне 88... 108 МГц, может быть использован любой бытовой радиоприемник, имеющий FM-диапазон (для отечественных приемников — диапазон УКВ-2). Единственным условием нормального приема является отсутствие (либо возможность отключения) системы автоматической подстройки частоты, в противном случае приемник будет перестраиваться от слабого сигнала радиозакладки на мощный сигнал ближайшей стационарной вещательной радиостанции.

**Специальные комплексы перехвата аудиосигналов**

Несмотря на многообразие закладных устройств и приемников излучений, особо следует отметить специальные комплексы перехвата речевой информации, тем более, что в последнее время такие средства профессионально выполняются на очень высоком уровне и представляют из себя технику нового поколения. Примером таких устройств могут служить цифровые системы передачи звуковой информации фирмы SIM Securiti & Electronic Sistem.
Model SIM-DST-100 — цифровая стереосистема передачи звуковой информации состоит из передатчика SIM-DST-100 и приемника SIM-DSR-100. Передатчик содержит два встроенных микрофона и блок питания в виде батареи. Передача звуковых сигналов в полосе от 40 Гц до 16 кГц осуществляется по двум каналам с тактовой частотой 32 кГц. Цифровое разрешение равно 16 бит. В передатчике применен код обнаружения и исправления ошибок. Выходная мощность передатчика равна 100 мВт.

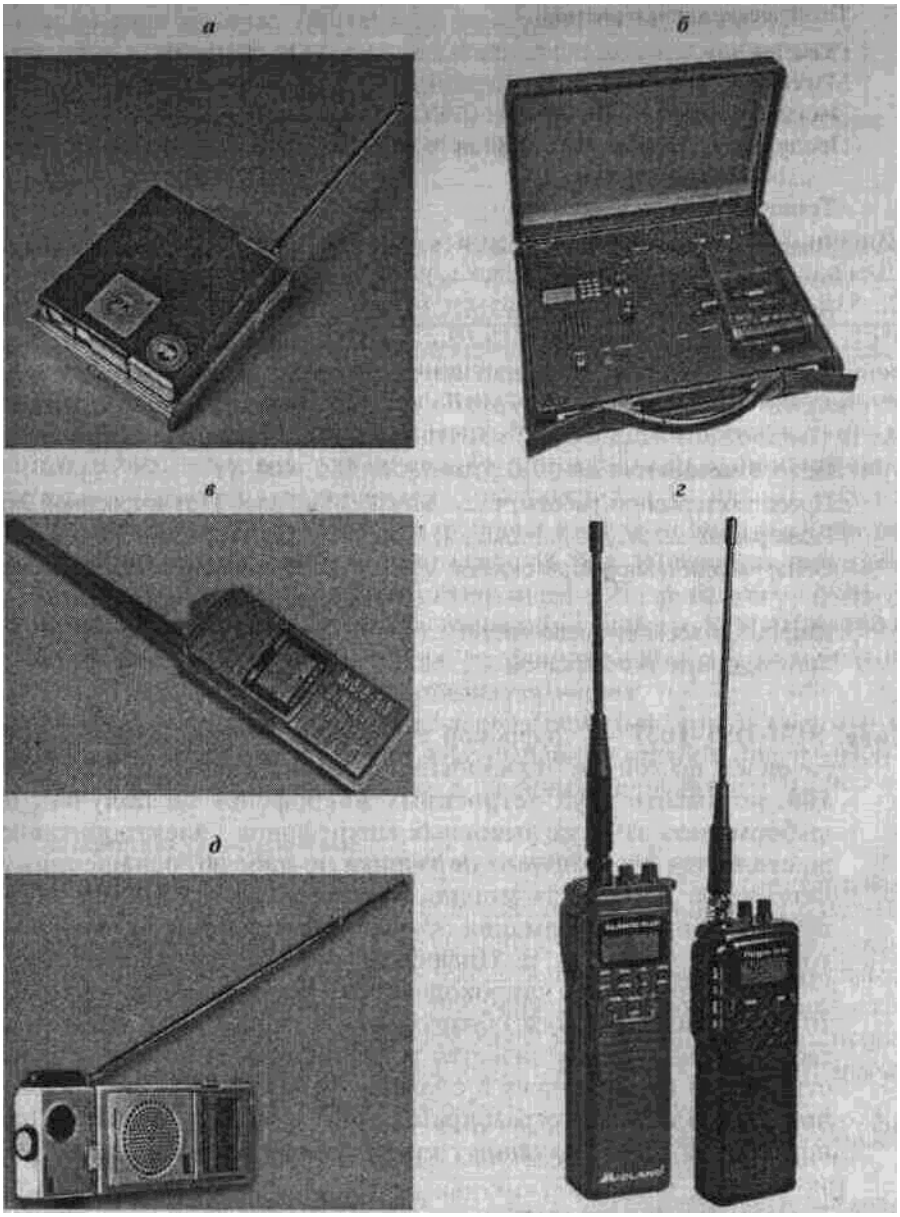



**Рис. 1.3.21. Специализированные, сканерные и другие устройства, применяемые для приема сигналов с радиозакладок:**
а — специальный приемник PK 255-SS; б — 100-канальный комплекс, размещенный в атташе-кейсе; в — панорамный радиоприемник AR 8000; г — портативные радиостанции; д — стандартная магнитола Panasonic со встроенным конвертором

Большим преимуществом аппаратуры данного типа является то, что радиосигналы передатчика могут быть приняты и декодированы только цифровым стереоприемником SIM-DSR-100. На выходе обычного аналогового радиоприемника, в том числе и аппаратуры контроля, получается белый шум без всяких признаков звуковой информации.

**Технические характеристики**

Диапазон частот, МГц ..... 890—980 (другие диапазоны по отдельным заказам)
Выходная мощность, мВт..... 100 (при напряжении электропитания 6 В)
Электропитание ..... встроенная батарея 6 В (возможно питание от внешних источников)
Потребляемый ток, мА..... 400
Продолжительность работы, ч..... более 3 (от встроенной батареи)
Размеры, мм..... 58x116x13
Обнаружение и коррекция ошибок ..... код обнаружения и исправления ошибок у источника

Ширина полосы звуковых частот..... 40 Гц —16 кГц
Тип соединителя с антенной ..... SMA

**Model SIM-DST-100F** — цифровой стереопередатчик **SIM-DST-100F** изготовлен по той же технологии, что и стереопередатчик **SIM-DST-100**, но вместо двух встроенных микрофонов он получает аудиоинформацию от двух выносных микрофонов. Электропитание осуществляется от внешнего источника по кабелю, оснащенному выключателем. Выходная мощность передатчика 100 мВт. Передача перехваченной информации осуществляется по двум каналам с тактовой частотой 32 кГц. Цифровое разрешение равно 16 бит.

Благодаря весьма широкой полосе передаваемых звуковых частот и применению кода обнаружения и исправления ошибок, достигается очень высокое качество воспроизведения перехваченного акустического сигнала даже в сложных условиях. Факт немаловажный при угрозе судебного разбирательства, а значит — проведения экспертизы по идентификации голосов участников разговора.

**Технические характеристики**

Диапазон частот, МГц ..... 890—980 (другие диапазоны по отдельным заказам)
Выходная мощность передатчика, мВт ..... 100 (при напряжении электропитания 6 В)
Электропитание ..... от внешнего источника постоянного тока 5—12В
Продолжительность непрерывной работы... зависит от типа источника электропитания
Размеры, мм..... 46x57x6
Микрофоны ..... два внешних
Ширина полосы звуковых частот ..... 40 Гц—16 кГц
Обнаружение и коррекция ошибок..... код обнаружения и исправления ошибок у источника
Тип соединителя с антенной ..... SMA

**Model SIM-DST-750** — цифровой стереопередатчик **SIM-DST-750** оснащен выносными микрофонами и обеспечен питанием от внешнего источника. Прибор обладает высокой выходной мощностью излучения (750 мВт), что обеспечивает большую дальность действия, и имеет прочную конструкцию.

Передача осуществляется по двум каналам с тактовой частотой 32 кГц. Цифровое разрешение равно 16 бит. Вследствие передачи со специальным кодированием передаваемые сигналы могут быть приняты и декодированы только стереоприемником **SIM-DSR-100.** На выходе обычного аналогового радиоприемника получится только белый шум без признаков аудиоинформации.

Благодаря широкой полосе передаваемых звуковых частот и применению кода обнаружения и исправления ошибок достигается высокое качество передачи даже в сложных условиях.

**Технические характеристики**

Диапазон частот, МГц ..... 890—980 (другие диапазоны по отдельным заказам)
Выходная мощность, мВт..... 750 (при напряжении
электропитания 6В)
Электропитание ..... от внешнего источника
постоянного тока 5—16В Потребляемый ток..... 400 мА
Продолжительность непрерывной работы... в зависимости от типа источника электропитания Микрофоны..... два выносных
Обнаружение и коррекция ошибок ..... код обнаружения и исправления ошибок у источника Ширина полосы звуковых частот, кГц.... 16
Размеры, мм..... 58x116x13

**Model SIM-DST-750** выпускается в следующих версиях: **DST-750 —** стандартная, с дистанционным управлением (диапазон УВЧ), а также с дистанционным управлением (диапазон УВЧ) и дополнительно с голосовой активацией.

**Model SIM-DSR-100** — портативный цифровой стереоприемник для приема и декодирования сигналов, передаваемых стереопередатчиками **SIM-DST-100** и **SIM-DSR-750.** Он имеет две разнесенные антенны и обеспечивает надежный прием даже при неблагоприятных условиях. Входная чувствительность приемника равна 94 дБ/мВт, ширина полосы звуковых частот — 16 кГц, цифровое разрешение — 16 бит.

При этих параметрах реальная дальность приема превышает типовую дальность действия системы. Приемник имеет цифровой выход для записи информации на ПЭВМ или, например, для подключения магнитофона с цифроаналоговым преобразователем ПАТ. Имеется также аналоговый выход. Помимо встроенной штатной магнитной антенны к приемнику можно подключать и внешние антенны других типов.

**Технические характеристики**

Диапазон частот, МГц ..... 890—980 (другие диапазоны по отдельным заказам)
Входная чувствительность ..... 94 дБ/мВт при ошибке по битам 10 бит
Количество каналов..... 12, предварительно настроенных
Точность настройки по частоте..... $\pm 20 \bullet 10^{-6}$
Стабильность настройки..... $\pm 50 \bullet 10^{-6}$ при температурах от -20° до + 50 °С)
Формат входных сигналов ..... линейная импульсно-кодовая модуляция, широкая полоса звуковых частот, цифровое разрешение 16 бит
Выходные сигналы ..... стереовыход, формат AES/EBU, тактовая частота 32кГц, 500 мВ (двойная амплитуда на сопротивление 750 Ом)
Электропитание, В..... 12, постоянный ток от внешнего источника
Размеры, мм..... 320x210x89
Коррекция ошибок ..... код обнаружения и исправления ошибок у источника

Для улучшения характеристик всех передатчиков указанных типов разработаны специальные антенны.

**Антенна Model SIM-SB-ANT** представляет собой оригинальную конструкцию, изготовленную с использованием современных материалов. Она может быть полностью помещена под одеждой и передавать сигналы практически без потерь. Антенна состоит из двух пластин, одна из которых располагается на груди, а вторая — на спине.

Пластины соединяются между собой проводом длиной 43 см, а с передатчиком —проводом длиной 60 см. Для диапазона частот 900— 960 МГц антенны имеют размеры около 190x100x1,6 мм. Наружные размеры пластин зависят от частот передачи (с понижением частоты они увеличиваются), но толщина их остается постоянной. Вокруг тела человека антенна создает равнонаправленное поле излучения без необлученных промежутков. Антенна этого типа может использоваться и как наружная, с установкой ее на жесткой опоре.

Полная масса антенны менее 30 г. Полоса пропускания равна б МГц. Стандартный диапазон частот 900—960 МГц (антенны для других диапазонов частот поставляются по отдельным заказам). Провод для соединения антенны с передатчиком имеет специальный штекер.

Кроме универсальных приемников и передатчиков аппаратура указанного типа выпускается в виде готовых комплектов «приемник-передатчик». Большим преимуществом таких систем является то, что они совершенно не требуют какой-либо предварительной взаимной настройки.

**Model SIM-CST-1000/CSR-1000** — управляемый микропроцессором миниатюрный передатчик аудиоинформации, оформленный в виде обычной электронной карточки, например для таксофона. Он имеет встроенные микрофон, батарею электропитания и антенну. К .передатчику может подключаться внешний микрофон специальным кабелем с соединителем и выключателем. Диапазон рабочих частот передатчика 1000—1100 МГц; выходная мощность на этих частотах до 1000 мВт. Опыт спецслужб показал, что данные устройства часто «пропускаются» даже при довольно тщательном личном досмотре.

По отдельному заказу передатчик поставляется с блоком голосовой активации (VOX) или со встроенными фильтрами верхних частот, переключающими передатчик на дежурный режим при отсутствии информации для передачи. Передаваемые сигналы кодируются и передаются в виде сигнала с импульсно-кодовой модуляцией. Управление передатчиком производится по специальной программе с помощью встроенного микропроцессора. Программа предусматривает настройку каналов передатчика и регулирование его выходной мощности.

**Приемник SIM-CSR-1000** также оформлен в виде карточки, в которую встроен миниатюрный декодер принимаемых сигналов.

**Технические характеристики**

Передатчик
Диапазон частот, МГЦ ..... 1000—1100, 8 каналов
Стабильность частоты..... $\pm 15 \bullet 10^{-6}$
Модуляция..... импульсно-кодовая
Микрофон..... встроенный или внешний (по дополнительному заказу)
Выходная мощность на радиочастотах, мВт .....100—1000, регулируется ступенями до семи уровней по программе или автоматически
Антенна..... встроенная

Передача сигналов звуковых
частот от микрофона..... один канал
Электропитание ..... литиевая батарея, потребляемый ток 50 мА
Продолжительность работы от батареи, ч ... 10—20
Потребляемый ток при работе с блоком VOX, мА..... 40
Масса, г ..... 20 (без батареи)
Размеры, мм.....:.... 86x54x3,8
Приемник
Стабильность настройки..... $\pm 200 \bullet 10^{-6}$
Чувствительность, мВ..... 2
Антенна..... шнур телефона
и телескопический штырь
Электропитание ..... батарея из двух элементов LR03 (AAA)
Потребляемый ток, мА.....25
Масса, г..... 40 (без батарей)
Размеры, мм..... 96x60x16

**Model SIM-DTX-500/DRX-500— DEC-500.** Передатчик речевой информации **SIM-DTX-500** может работать в режиме открытой передачи в диапазоне СВЧ с узкополосной частотной модуляцией или в режиме цифрового кодирования со скоростью передачи 40 кбайт/с. Настройка передатчика производится вручную с шагом 5 кГц. Передатчик имеет соединитель с внешним микрофоном.

**Приемник SIM-DRX-500** сканирующего типа имеет встроенную плату декодера **SIM-DES-500.** Имеется вариант приемника с декодером в виде отдельного блока. Возможна модификация приемника в соответствии с требованиями заказчиков.

**Технические характеристики**

Передатчик
Диапазон частот, МГц ..... 165—174
Настройка ..... ручная с шагом 5 кГц,
Режимы работы..... с узкополосной частотной
модуляцией или с цифровым кодированием сигналов
Микрофон..... внешний, миниатюрный
Конденсаторный Выходная мощность, мВт..... 100—500 (регулируется вручную)
Кодер сигналов низкой частоты..... аналого-цифровой преобразователь с сигма-дельта модуляцией
Электропитание ..... источник постоянного тока, 9 В
Потребляемый ток, мА..... 200 (макс.)
Размеры, мм..... 38x4x78
Приемник
Тип ..... портативный сканерного типа
Выход звуковых частот..... 32 мВт, на головные телефоны или в линию

**Model SIM STEALTH.** Стереосистема **SIM STEALTH** состоит из цифрового стереопередатчика звуковых частот и приемника. По дополнительному заказу передатчик может быть поставлен в версии с дистанционным управлением. Для увеличения дальности действия в системе применяется ретранслятор. Однако даже без помощи последнего дальность действия цифрового стереопередатчика достигает 500 м. Он питается от внешних источников постоянного тока и может устанавливаться скрытно. Версия передатчика с дистанционным управлением имеет дополнительный приемник команд для приема сигналов управления. Вся передаваемая аудиоинформация кодируется для защиты от непреднамеренного перехвата. Примененный метод модуляции создает для таких случайных слушателей только белый шум, из которого невозможно не только извлечь информацию, но и установить сам факт передачи. Полоса частот звуковых сигналов равна 16 кГц, это обеспечивает их передачу с высоким качеством.

Приемник работает от встроенных батарей или с помощью внешнего блока питания от электросети. Он имеет клавиатуру управления и жидкокристаллический дисплей. В версии системы с дистанционным управлением можно из удаленного пункта включать и выключать передатчик, регулировать выходную мощность и подправлять настройку. Данные в канале дистанционного управления передаются в определенном нестандартном формате. При применении специального кода приемник может последовательно принимать сигналы до 100 передатчиков. Постоянная настройка может быть произведена

предварительно на частоты четырех передатчиков.
Подстройка на частоту передатчика производится автоматически, но может выполняться и вручную.
Ретранслятор имеет такую же конструкцию, как и приемник. Он принимает сигналы передатчиков с цифровым кодированием информации и не только передает их с усилением мощности, но при этом производит преобразование частот сигналов в более высокие. Дальность передачи с применением ретранслятора может быть увеличена до 3—5 км без ухудшения качества.
Система **SIM STEALH** выпускается в нескольких версиях:
**STEALTH-NRC —** без дистанционного управления; режимы передачи моно- или стерео; компоненты: передатчик NRC, приемник NPC;
**STEALTH-RCA** — с дистанционным управлением; **режим** передачи моно- или стерео; компоненты: передатчик **RC**, приемник **RC**;
**STEALTH-Relay-NPC** — без дистанционного управления; режимы передачи моно- или стерео с ретрансляцией; компоненты: передатчик NRC, приемник NRC, ретранслятор;
**STEALTH-Relay-RC** — с дистанционным управлением; режимы передачи моно- или стерео с ретрансляцией; компоненты: передатчик **RC**, приемник RC, ретранслятор.
**Технические характеристики**
Передатчик (модели NRC-TX и RC-TX)
Дистанционное управление ..... только RC-TX
Система передачи аудиоинформации..... стерео
Диапазон частот, МГц
прямая передача ..... 360—375 (шаг перестройки 100 кГц)
с ретрансляцией..... 320—335 (шаг перестройки 100 кГц)
Фиксированная частота настройки командного приемника, МГц ..... 172,5
Стабильность частоты передатчика, кГц... лучше ±15
Выходная мощность на радиочастотах.... программируется с изменением по восьми уровням, макс. 100мВт
Подавление гармоник, дБ ..... лучше - 30
Полоса пропускания ..... 200 кГц — 1 МГц
Обработка сигналов ..... цифровое кодирование со скремблированием; два канала звуковых частот
Скорость передачи, кбайт/с ..... 200
Модуляция сигналов звуковых частот.... четырехуровневая частотная манипуляция(F6)
Ширина полосы звуковых частот..... 200 Гц—12 кГц
Динамический диапазон ..... более 6 дБ при искажениях до 5%
Уровень шумов в системе ..... ниже 2 мВ, ограничивается применением специальных микрофонов
Усилитель звуковых частот, дБ ..... 35
Электропитание ..... источник постоянного тока, 8—30 В
Потребляемый ток, мА..... 60 при 6 В, 20 при 30 В
Продолжительность непрерывной работы, ч.. 100 при выходной мощности 100 мВт, 400 при выходной мощности 1 мВт
Диапазон рабочих температур, °С ..... от-10 до+60
Размеры, мм..... 54x4,7x73
Приемник
Аудиосистема..... стерео
Диапазон частот, МГц 360—375 (с шагом
перестройки 100 кГц) Выходная мощность на высоких частотах, мВт..... 100
Подавление гармоник, дВ..... -60
Скорость выдачи данных, Бод ..... 464
Длительность принимаемых сигналов, с... 5
Электропитание ..... источник постоянного тока 12
Потребляемый ток, мА..... 12 в дежурном режиме, 240 при приеме
Стабильность частоты, кГц..... лучше ±10
Чувствительность, дБ/мВт..... -110
Полное сопротивление антенны. Ом ..... 50, соединитель BNC
Уровень гармоник гетеродина, дБмВт.... ниже -70
Уровень шума, дБ ..... ниже 3

Усиление по промежуточной частоте, дБ.. 17
Ширина полосы пропускания, кГц..... 250
Продолжительность непрерывной работы, ч.. 2
Размеры, мм..... 300x80x320

**Model SIM-DSS-2000. SIM-DSS-2000** — система с использованием широкополосных (spread spectrum) сигналов для передачи аудиоинформации. Так как энергия передаваемых сигналов распределяется по широкому спектру, работу системы очень трудно обнаружить без применения специальной аппаратуры радиоразведки и вероятность перехвата сигналов мала. Эта очень дорогая и сложная система предназначена для использования международными и национальными силами полиции и службами безопасности.

Цифровой миниатюрный стереопередатчик с дистанционным управлением передает сигналы на близлежащую портативную, подвижную или стационарную радиостанцию. Принятые этими станциями сигналы декодируются и прослушиваются с использованием головных телефонов или громкоговорителя и могут одновременно записываться магнитофоном.

В системе SIM-DSS-2000 применена прямая модуляция несущей частоты передаваемым информационным сигналом в сочетании с псевдослучайной последовательностью, в результате чего энергия радиочастотного сигнала (мощность 300 мВт) распределяется в полосе спектра шириной до 10 МГц. Это значит, что система становится как бы «невидимой» для стандартных средств перехвата, и вероятность перехвата близка к нулю. Ширина занимаемой полосы спектра регулируется с использованием блока дистанционного управления так, чтобы исключить возможность помехи от сильных широкополосных сигналов, например, мощных телевизионных передатчиков.

Для большей защищенности от перехвата аудиосигналы еще до модуляции несущей частоты шифруются, что исключает возможность их быстрого «смыслового» раскрытия потенциальными перехватчиками, даже при обнаружении факта прослушивания. Пользователь может в любое время заменить ключ шифрования, передав соответствующую команду через блок дистанционного управления.

Испытания системы показали, что ее передачи практически невозможно принимать обычными радиоприемниками. Кроме того, оператор может дистанционно снижать выходную мощность на радиочастотах до минимального уровня, допустимого при заданной дальности передачи.

Если передатчик используется как носимый на теле агента, то в критических ситуациях оператор может воспользоваться имеющимися на передатчике кнопками «тревога» (panic) и «прекращение передачи» (delay off), предназначенными для его защиты. При нажатии кнопки «тревога» приемник системы SIM-DSS-2000 принимает сигнал тревоги. Кнопка «прекращение передачи» дает возможность оператору экстренно выключать передатчик. При этом другие устройства автоматически включают сигнал тревоги.

Передатчик имеет два независимых канала, по которым в него поступает подлежащая передаче аудиоинформация. Эти микрофоны пространственно разнесены, и воспринимаемые ими звуки создают полное представление об обстановке в контролируемом помещении.

Применяемый код обнаружения и коррекции ошибок у источника обеспечивает достоверную передачу при сохранении хорошей разборчивости даже при неблагоприятных условиях.

Приемное устройство и блок дистанционного управления объединены и оформлены в виде миниатюрного цифрового стереоприемопередатчика **SIM-DSS-2000R**, который можно носить в портфеле типа «дипломат», под одеждой или использовать в подвижном варианте.

Этот приемопередатчик принимает широкополосные радиосигналы, демодулирует и дескремблирует (производит «свертку» по частоте) их. Прием может осуществляться в широком диапазоне радиочастот и от нескольких передатчиков, работающих на одной частоте с применением многократного доступа с кодовым разделением МДКР (CDMA). Пакетный передатчик команд этого блока предназначен для дистанционного управления передатчиков **SIM-DSS-2000.**

Пользователь может предварительно выбрать набор регулируемых параметров или один параметр передатчика, значения которых и устанавливаются по командам дистанционного управления. В приемопередатчике применен код обнаружения и исправления ошибок на выходе приемника. На лицевой панели управления приемопередатчика расположены светодиодные индикаторы состояния приемника и передатчика, дисплей на четыре знакоместа и переключатели быстрого изменения параметров системы.

Блок SIM-DSS-2000R имеет выходы на головные стереотелефоны и аудиомагнитофон.

**Технические характеристики комплекса**

Передатчик
Диапазон частот, МГц ..... 849,92—952,32 400—450
Выходная мощность, мВт..... 300 (макс.)
Регулирование выходной мощности, мВт .... от 0 до 3 с шагом 0,3, от 3 по 400 с шагом 1
Модуляция ..... спектральная, с использованием псевдослучайной последовательности и получением широкополосных (псевдошумовых) сигналов
Вид передачи ..... многоканальная с частотным и кодовым разделением каналов
Количество каналов с частотным разделением ..... 21
Частотный интервал между каналами, МГц ..... 5,12
Ширина полосы канала, МГц..... 16
Стабильность частоты..... $\pm 1{,}5 \bullet 10^{-6}$ (при температурах от-30 до+60 °С)
Антенна ..... входное сопротивление 50 Ом, соединитель SMA
Код обнаружения и коррекции ошибок.... сверхточный код «Витерби» с отношением 1:2
Усиление при коррекции ошибок, дВ ... 5,2
Ширина полосы звуковых частот ..... 150 Гц—7 кГц
Количество каналов передачи сигналов звуковых частот от микрофонов ...2
Разделение каналов,дБ..... более 70
Динамический диапазон, дБ ..... более 70
Напряжение входного сигнала от микрофонов, мВ ..... 10
Электропитание микрофонов..... постоянный ток, 4В
Полоса частот голосовой активации (VOX), Гц ..... 300—1200
Несущая частота канала передачи команд дистанционного управления, МГц.... 400
Мощность сигналов дистанционного управления, Вт..... 5 (макс.)
Скорость передачи сигналов
дистанционного управления, кбит.... 2,3
Выключение (голосовой активацией) .... от 200 мс до 10 с (регулируется)
Электропитание ..... источник постоянного тока, 6 В от (4,5 до 6 В)
Потребляемый ток, мА..... 10 (дежурный режим) 160—350, при выходной мощности 0—99 %
Подавление гармоник, дБ ..... лучше 25
Диапазон рабочих температур °С ..... от -20 до +60
Размеры, мм..... 82,5 (94 с антенным соединителем SMA)x53,2x19,2
Приемник
Коэффициент шума, дБ..... 7
Чувствительность, дБ/мВт..... -105
Динамический диапазон, дБ ..... более 95
Стабильность частоты настройки ..... $\pm 1{,}5 \bullet 10^{-6}$ (при температурах
от 30 до+60 °С
Антенна
Входное сопротивление..... 50 Ом с соединителем TNC
Время синхронизации, с..... менее 1
Выходная мощность блока
дистанционного управления, Вт.... 5, макс. (регулируется)
Подавление гармоник, дБ ..... лучше-60
Выход на головные телефоны..... 1,2В (макс.) на сопротивлении 10 Ом
Выход на аудиомагнитофон или линию..... 1 В (макс.) на сопротивлении 2 кОм
Канал дистанционного управления..... интерфейс RS232, скорость передачи 115 200 кбит/с
Электропитание ..... постоянный ток, 12 В (9—15В)
Потребляемый ток, мА..... 22 — дежурный режим, менее 700 при синхронизации
Защита электропитания..... от перемены полярности и перегрузок Размеры, мм..... 61x145x221

**Комплекс Model** SIM-DSS-5000. Приемопередатчик SIM-DSS-5000T с псевдослучайной скачкообразной перестройкой несущей частоты (Frequency hopping) и широкополосными (шумоподобными) сигналами отличается высокой защищенностью информации от перехвата. Он предназначен для использования международными и национальными силами полиции и служб безопасности.

Для снижения вероятности перехвата передаваемые сигналы звуковых частот

преобразуются в цифровую форму и шифруются еще до модуляции. Пользователь может в любое время сменить ключ шифра посредством передачи соответствующей команды через блок дистанционного управления.
Проведенные испытания системы показали, что ее передачи практически невозможно принимать с помощью обычных радиоприемников. Кроме того, оператор может, пользуясь блоком дистанционного управления, снижать выходную мощность передатчика до минимальной, обеспечивающей требуемую дальность передачи.
При использовании в нательном варианте, в критических ситуациях оператор может воспользоваться имеющимися на передатчике кнопками «тревога» (panic) и «прекращение передачи» (delay off). При нажатии кнопки «тревога» приемник системы принимает сигнал, включающий устройство тревожной сигнализации. Кнопка «прекращение передачи» дает возможность оператору выключить электропитание передатчика, вследствие чего излучение прекращается. При всяком выключении электропитания, вызванном другими причинами, включается сигнал тревоги.
Передатчик имеет два независимых канала приема сигналов звуковых частот от двух микрофонов. Пространственное разнесение этих микрофонов создает некоторое представление об обстановке в контролируемом помещении.
Применение кода обнаружения и коррекции ошибок у источника сигналов обеспечивает достоверность передачи при сохранении хорошей разборчивости.
Излучаемые всенаправленной антенной цифрового стереопередатчика сигналы принимаются расположенной поблизости портативной подвижной или неподвижной станцией. Принятые сигналы декодируются и могут прослушиваться через головные телефоны или громкоговоритель и записываться с помощью магнитофона.
Несущая частота передатчика скачком изменяется 500 раз в 1 с в пределах полосы 100 МГц, вследствие чего энергия сигнала распределяется в полосе спектра 10 МГц на каждой новой частоте. Поэтому вероятность перехвата сигнала близка к нулю.
Несущая частота передатчика может выбираться пользователем в пределах диапазонов 850—950 или 750—850 МГц. Это дает возможность исключить помехи от источников мощных широкополосных сигналов, например от передатчиков телевидения.
Приемное устройство и блок дистанционного управления передатчиком **SIM-DSS-5000T** оформлены, как и отдельный цифровой сте-реоприемопередатчик **SIM-DSS-50000R**, в прочном корпусе. Его можно носить в портфеле типа «дипломат», под одеждой или использовать в подвижном варианте. Этот приемопередатчик может принимать сигналы в широком диапазоне радиочастот от нескольких передатчиков **SIM-DSS-5000T**, работающих на одной и той же частоте с многократным доступом с кодовым разделением MDKP (CDMA). Принятые широкополосные радиосигналы демодулируются и дескремблируются, а выделенные сигналы звуковых частот декодируются. Система дистанционного управления передает команды на передатчик **SIM-DSS-5000T** в форме коротких пакетов. Пользователь может предварительно выбрать полный набор значений регулируемых параметров передатчика.
На панели управления приемопередатчика имеются светодиодные индикаторы состояния и дисплей на четыре знако-места, а также переключатели для быстрого изменения параметров системы. Приемник имеет выходы на головные стереотелефоны и магнитофон.

**Технические характеристики**

Передатчик
Вид передачи ..... с псевдослучайной скачкообразной перестройкой несущей частоты
Диапазоны частот, МГц ..... 850—950, 750—850
Количество скачков (изменений) частоты в 1с..... 500
Ширина полосы скачкообразной перестройки несущей, МГц ..... 100
Управление скачкообразной перестройкой..... случайная последовательность импульсов Выходная мощность, мВт..... 300
Регулировка выходной мощности, мВт ... 0—3 с шагом 0,3
3—300 с шагом 3
Антенна, Ом, ..... входное сопротивление 50, соединитель SMA
Количество каналов передачи звуковых частот от микрофонов ..... 2
Разделение каналов, дБ..... более 70
Динамический диапазон, дБ ..... более 7
Ширина полосы звуковых частот..... 150Гц—7 кГц

Полоса звуковых частот голосовой активации, Гц..... 300—1200
Скорость передачи команд дистанционного управления, кбит/с..... 2,3
Режим передачи команд дистанционного управления..... пакетный
Длительность пакета, мс ..... менее 100
Выключение голосовой активацией .... от 200 мс до 10 с
(регулируется)
Электропитание ..... постоянный ток, 6 В
(4,5-6,5 В)
Потребляемый ток, мА..... 4—дежурный режим, 100—350—передача (с выходной мощностью 0—99%)
Защита питания..... от перенапряжений
Приемник
Чувствительность, дБм/Вт ..... -150
Динамический диапазон, дБ ..... более 95
Стабильность частоты настройки ..... $\pm 1{,}5 \bullet 10^{-6}$ (при температурах от 0°до+60°С)
Антенна..... входное сопротивление 50 Ом, соединитель TNC
Выход на головные телефоны, В ..... 1,2 (макс.) на сопротивлении 10 0м
Выход на магнитофон или линию, В ..... 1 (макс.) на сопротивлении 2к0м
Канал дистанционного управления..... интерфейс К8232,скорость передачи 115 200кбит/с
Электропитание ..... постоянный ток, 12 В (9—15В)
Защита электропитания..... от перемены полярности и перегрузок Диапазон рабочих температур, °С ..... от 0 до +50
Размеры, мм..... 61х145х22
Рассмотренные выше системы достаточно надежно защищены от комплексов контроля радиоизлучений, предназначенных для выявления радиозакладок, принцип действия которых будет подробно рассмотрен в разделе 2.3. Однако и такие закладки могут быть выявлены при правильном построении системы безопасности предприятия.

**1.3.2. Закладные устройства с передачей информации по проводным каналам**

Техническая возможность применения токоведущих линий для передачи перехваченной акустической информации практически реализована в целом ряде ЗУ. Наиболее широкое распространение получили закладки, использующие для этих целей сеть 220 В.
Типовая схема организации негласного прослушивания переговоров с задействованием энергосети приведена на рис. 1.3.22.
Как правило, подслушивающие устройства устанавливаются в стандартную розетку или любой другой постоянно подключенный к силовой сети электроприбор (тройник, удлинитель, блок питания радиотелефона, факс и т. д.), расположенный в помещении, в котором ведутся переговоры интересующих лиц. Типовая схема такой закладки приведена на рис. 1.3.23.
Чувствительность внедренных микрофонов, как правило, обеспечивает надежную фиксацию голоса человека или группы лиц на удалении до 10 м.

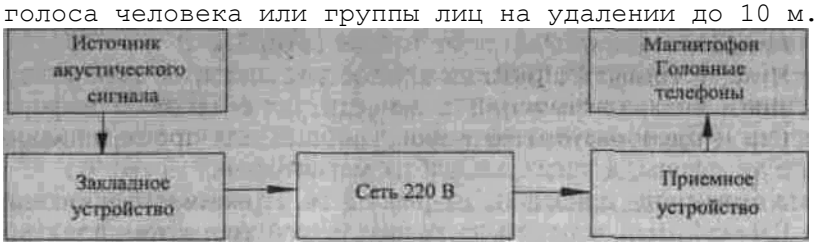



**Рис. 1.3.22. Схема применения закладного устройства с передачей информации по сети 220 В**

Дальность передачи информации лежит в пределах от 300 до 1000 м. Она обеспечивается за счет применения выходного усилителя с мощностью 5...300 мВт и амплитудной или частотной модуляции несущей, специально сформированной в задающем генераторе закладного устройства. Несущая модулируется информационным сигналом, прошедшим предварительное усиление в низкочастотном (НЧ) усилителе, и через высокочастотный (ВЧ) усилитель и специальное согласующее устройство излучается в линию. Частота передаваемого сигнала лежит в диапазоне 50... 300 кГц. Выбор данного участка обусловлен тем, что, с одной стороны, на частотах ниже 50 кГц в сетях электропитания относительно высок уровень помех от бытовой техники, промышленного

оборудования, лифтов и т. д. С другой — на частотах выше 300 кГц существенно затухание сигнала в линии, и кроме того, провода начинают работать как антенны, излучающие сигнал в окружающее пространство. Однако в некоторых случаях используются колебания с частотами, достигающими 10 МГц.


**Рис. 1.3.23. Структурная схема закладного устройства**

Питание ЗУ осуществляется от той же сети, 220 В.

Приемное устройство, расположенное вне пределов контролируемого помещения и подключенное к той же сети, перехватывает информационный сигнал и преобразует его в вид, удобный для прослушивания через головные телефоны, а также запись на магнитофон.

Схема приемника приведена на рис. 1.3.24. Принимаемый сигнал поступает на ВЧ-усилитель через согласующее устройство, затем детектируется и через НЧ-усилитель подается на головные телефоны или магнитофон. Чувствительность такого устройства, как правило, лежит в пределах от 3 до 100 мкВ, а питание осуществляется от батареек (аккумуляторов).

В некоторых случаях для одновременного прослушивания нескольких помещений используются многоканальные системы. При этом ЗУ работают на различных фиксированных частотах, а оператор выбирает на приемном устройстве канал, необходимый для прослушивания в каждый конкретный момент времени (рис. 1.3.25, а).

В целом устройства контроля акустической информации с передачей по сети 220 В обладают существенными преимуществами перед другими ЗУ. Так, например, по сравнению с радиозакладками — повышенной скрытностью (поскольку невозможно ее обнаружение с помощью радиоприемных устройств), а также практически неограниченным временем непрерывной работы, так как не требуют периодической замены источников питания. По сравнению с обычными проводными микрофонами (рис. 1.3.25, б), использующими собственные проводники для передачи сигнала, — практически невозможно точно выявить место установки приемного оборудования.

Однако при использовании данной техники возникают существенные проблемы.

Во-первых, работа возможна только в пределах одной фазы электропроводной сети.

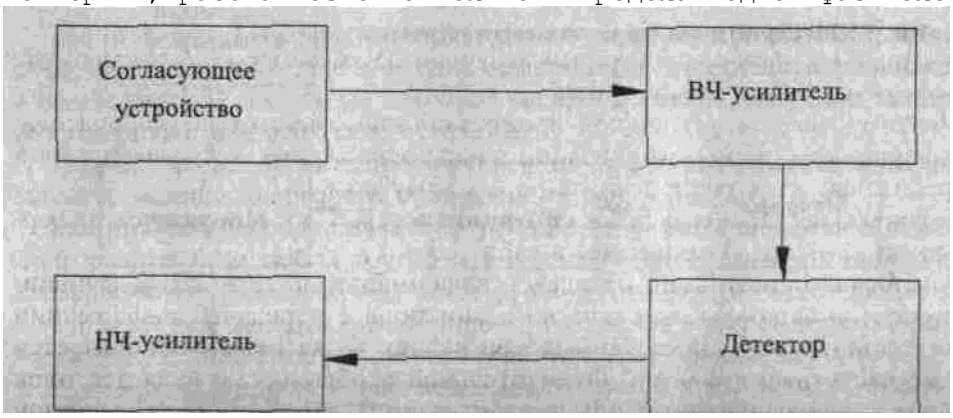


**Рис. 1.3.24. Структурная схема приемного устройства**

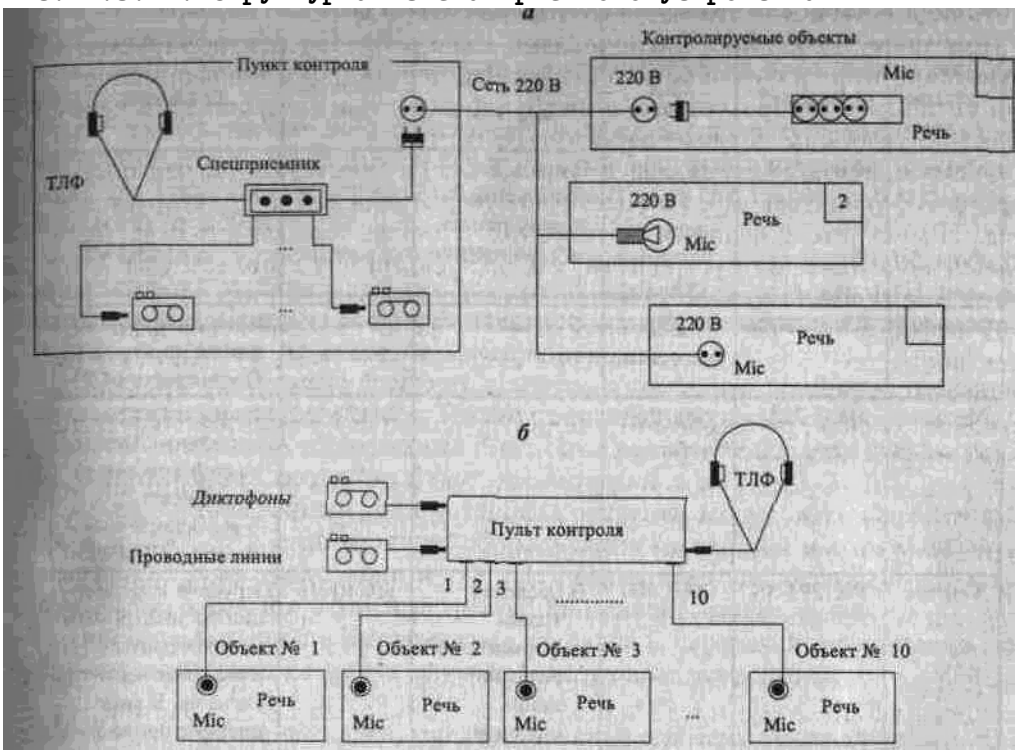



**Рис. 1.3.25. Многоканальные закладные устройства с передачей информации на пункт сбора и обработки по токоведущим линиям:**

а — по сети 220 В; б — по специально проложенным кабелям

Во-вторых, на качество перехватываемой информации влияют различные сетевые помехи.

В-третьих, прибор, в который внедрено ЗУ, может быть случайно отключен от сети переменного тока.

Поэтому применение данной техники обычно сопровождается тщательным изучением схемы организации электроснабжения, наличия и типов потребителей электроэнергии, выбором камуфляжа.

Технические характеристики некоторых сетевых ЗУ с передачей информации по сети 220 В приведены в табл. 1.3.3.

Аналогично системам с передачей информации по сети 220 В функционирует и аппаратура акустического контроля с передачей информации по телефонной сети. В состав изделий входят те же блоки, используется тот же частотный диапазон. Отличительной особенностью является блок питания, предназначенный для преобразования напряжения телефонной линии к требуемому уровню. В связи с тем, что от телефонной линии

**Таблица 1.3.3. Основные характеристики сетевых закладных устройств**

| Вид исполнения | Индекс | Частота, МГц Вид модуляции | Дальность действия, м | Габариты, мм | Примечание |
|---|---|---|---|---|---|
| Модуль | РК1295-S | 60...200 Узкополосная частотная (±6 кГц) | В пределах трансформаторной развилки линии питания | — | — |
| Модуль | «Сеть 2НК» | 100 Частотная | 200 | — | Передача информации по электросети. В комплекте с ПРМ |
| Модуль | НКG-2221 | 120...260 Частотная | 100 | 67×3 ×25 | Микрофон с компрессором. Передача информации по электросети. 6 закладок в комплекте с ПРМ |
| Модуль | РК1295-SS | 200...400 | В пределах трансформаторной развилки линии питания | 60×40×16 | Передача информации по электросети. Скачкообразное изменение частоты сигнала. В комплекте с приемником. Выносной микрофон. Потребляемая мощность 100 мВт |
| Сетевой удлинитель | «Сеть 2Ч» | _____ Частотная | 200 | — | Передача информации по электросети. В комплекте с приемником. Потребляемая мощность 100 мВт |
| Сетевая розетка | «Сеть IP» | _____ Частотная | 100 | — | То же |
| Модуль | УЗПИ | _____ Узкополосная частотная (±3,5 кГц) | В пределах трансформаторной развилки линии питания | 110×70×25 | То же |

нельзя потреблять более 2 мА, мощность передающих устройств не может превышать 10...15 мВт.

Однако существуют определенные ограничения на применение подобных устройств.

Во-первых, необходимо подключать приемную аппаратуру именно к той телефонной линии, на которой установлено устройство съема информации, что упрощает обнаружение пункта контроля (по сравнению с передачей по сети 220 В).

Во-вторых, устройство достаточно габаритное и его относительно трудно использовать скрытно, так как все возможные места установки (телефонный аппарат, розетки, распределительное оборудование и т. д.) легко проверить, в отличие от системы электропроводки.

Вышеперечисленные факторы привели к тому, что данные устройства практически не используются. Иные (широко применяемые) способы и устройства для съема информации с использованием телефонов и коммуникационных линий подробно будут рассмотрены в п. 1.5.2.

Подобно телефонным, для установки закладок могут быть использованы и другие сети слаботочного оборудования (пожарной и охранной сигнализации, радиотрансляции и т. д.). Их недостатки аналогичны приведенным выше, в связи с этим и реальное применение крайне редко.

Примерами серийно выпускаемых закладок с передачей информации по токоведущим линиям

могут служить следующие устройства:
**UM104** — сетевая закладка, предназначенная для прослушивания служебных и жилых помещений путем передачи и приема акустической информации по сети переменного тока. Дальность передачи (по проводам) — не менее 30 м; словесная разборчивость (при отсутствии помех) — 90 %; электропитание закладки — сеть 220 В; питание приемника — 4 батареи «АА».
Закладка устанавливается вместо стандартной стенной розетки или встраивается в электробытовые приборы. При установке в нишу стенной розетки UM104 полностью выполняет все ее функции и допускает подключение электроприборов мощностью 1,5 кВт. Отличительной способностью спецприемника является подключение к силовой сети только одним проводом, что обеспечивает повышенную безопасность и удобство в эксплуатации. Выбор провода для подключения определяется небольшим экспериментом и по лучшему качеству прослушивания. Контроль переговоров разрабатываемых лиц ведется на головные телефоны.
**IPS MCX** — акустическая закладка с передачей информации по сети переменного тока. Скрытно устанавливается в одном из бытовых приборов. Диапазон используемых для передачи частот — до 120 кГц; рабочее напряжение 100...260В переменного тока с частотой 50/60 Гц-диапазон передаваемого акустического сигнала— 300...3500Гщ модуляция — узкополосная частотная; габариты — 33х67х21 мм.
Передаваемая информация принимается приемником, рассчитанным на обслуживание шести передатчиков. Он оборудован встроенным громкоговорителем и выходами на диктофон и головные телефоны. Для записи на магнитофон имеется линейный выход.
**PK170** — телефонная закладка с рабочей частотой около 100 кГц, вес — 180 г, габариты — 130х30х20 мм. Используется частная модуляция. В комплекте поставляется приемник (вес 750 г). Закладку производитель рекомендует устанавливать либо непосредственно в телефонном аппарате, либо в телефонной розетке.
**Model SIM-ROTEL** — представляет собой приемник звуковых сигналов от микрофонов устройств подслушивания (закладок), установленных в контролируемых помещениях или в телефонных аппаратах и линиях. Он может одновременно принимать сигналы от четырех таких микрофонов. Чувствительность каждого канала приема можно регулировать отдельно. Микрофоны, включенные в телефонную линию, включаются автоматически при переходе телефона в режим приема или передачи сигналов вызова.
Приемник **SIM-ROTEL** имеет два отдельных выхода принятых сигналов звуковых частот для их обработки или регистрации. Прием информации с микрофонов, включенных в телефонную линию, не создает в ней никаких помех, по которым мог бы быть обнаружен факт перехвата информации. Таким образом, любимая тема для пересудов некоторых «знатоков», когда они слышат в линии какой-нибудь посторонний щелчок, в данном случае отпадает. Приемник может вводить в линию напряжение, компенсирующее падение напряжения в ней, вызванное подключением микрофонов. Каждый микрофон может включаться и выключаться дистанционно.
Приемник **SIM-ROTEL** в сочетании со скрыто устанавливаемыми микрофонами образует гибкую систему перехвата звуковой информации, которая может быть использована для мониторинга не только любых аналоговых телефонных линий, но и других двухпроводных линий. В стандартный комплект входят два микрофона - и один приемник.
**Технические характеристики**
Электропитание, В..... сеть переменного тока, 220 (по отдельному заказу—110)
Компенсация падения напряжения в линии .. активная, 35—65 В, 15 мА
Каналы приемника..... два канала приема сигналов от
микрофонов + канал приема от телефонной линии.
Чувствительность каждого канала регулируется отдельно Выходы приемника ..... для выхода на линии передачи, один выход на головные телефоны с индивидуальной регулировкой громкости
Потребляемый одним микрофоном ток, мА. 1,8 при напряжении 40 В
Выходная мощность звуковых частот .... более 60 мВт, 0,5 В (двойная амплитуда на сопротивлении 600 Ом (типовая)
Дальность передачи по линии, км ..... до 3
Полоса звуковых частот..... от 20 Гц до 5 кГц
Передача сигналов по линии..... с амплитудной модуляцией на разных несущих в диапазоне 30—200 кГц

**Model SIM-ОСИ, SIM-OC21** — эти системы содержат передатчики **SIM-OC11T и SIM-OC21T** и приемники **SIM-OC11R и SIM-OC21R.** Передача сигналов производится по проводам электросетей, которые используются также для электропитания самого прибора. Автоматическая регулировка усиления позволяет принимать все разговоры в контролируемых помещениях с высокой разборчивостью. Для достижения большей скрытости перехвата вся передаваемая звуковая информация предварительно подвергается цифровому кодированию.

Передатчик **SIM-OC11T** снабжен трехжильным кабелем, который может быть подключен к электросети в любом месте. Если электросеть имеет «нулевую» фазу, дальность передачи может быть увеличена. Чувствительность каждого микрофона регулируется отдельно.

Приемник **SIM-OC11R** декодирует, принимаемые сигналы. На лицевой панели этого приемника расположены выходы на головные телефоны, громкоговоритель (с регулировкой громкости) и на магнитофон.

Система, укомплектованная передатчиком **SIM-OC21T** и приемником **SIM-OC21R**, может управляться дистанционно и передавать код идентификации передатчика **OC-2IT** длиной 3 бит.

**Технические характеристики**

Модуляция..... амплитудная
Выходная мощность, мВт..... 300 на сопротивлении 10 Ом
Защита передаваемых сигналов..... цифровое кодирование
Электропитание, В ..... сеть переменного тока 220—240
Чувствительность, мкВ ..... 500
Отношение сигнал/шум, дБ..... 45 или выше
Ширина полосы звуковых частот, Гц..... 100—3 000
Уровень сигнала на выходе для магнитофона ... более 50 мВ на сопротивлении 1 кОм
Светодиодный индикатор состояния ..... красное свечение — приемник включен, зеленое свечение — прием сигналов
Размеры, мм:
SIM-OC11T..... 21x31x66
SIM-OC21T..... 27x31x66
SIM-OC11R..... 40x65x120
SIM-OC21R..... 40x110x120

**Model SIM-RMM** специально предназначена для скрытого мониторинга помещений и телефонов с использованием имеющихся телефонных линий. Все разговоры в помещениях и по телефону могут перехватываться, записываться и передаваться в удаленный пункт. Система SIM-RMM использует принципиально новую технику, которая ранее не применялась при мониторинге в коммутируемых телефонных сетях общего пользования.

Система состоит из двух модулей, входного модуля передатчика для мониторинга разговоров в помещении и модуля приемника с усилителем сигналов, перехватываемых в телефонных линиях.

Модуль передатчика комплекса SIM-RMM содержит высокочувствительный микрофон, соединенный с усилителем звуковых частот, имеющим широкий динамический диапазон, быстродействующую автоматическую регулировку усиления и защищенный от перегрузок при скачках в сети электропитания и появлении сигналов вызова в телефонной линии.

Этот модуль контролирует разговоры в помещении, где установлен телефон при неснятой трубке телефонного аппарата. При снятии трубки модуль RMM переключается на контроль телефонных переговоров. Модули передатчика доступны в различных вариантах, включая версии со скремблированием сигналов.

Модуль приемника SIM-RMM заключен в прочный алюминиевый корпус и содержит усилитель перехваченных сигналов с высоким входным сопротивлением и фильтрацией помех для получения максимально возможного отношения сигнал/шум. Имеются версии этого модуля с дескремблированием принимаемых сигналов. Приемник имеет выход на головные телефоны с выключателем голосовой активации и сбалансированный выход с сопротивлением 600 Ом для ретрансляции сигналов по стандартным линиям коммутируемой телефонной сети общего пользования или линии МККТТ М1 200.

**Технические характеристики**

Модуль передатчика
Выходное напряжение, мкВ ..... 400 на сопротивлении 12000м

Ширина полосы звуковых частот, Гц..... 100—3500
Потребляемый ток, мА..... 3 (постоянный ток)
Автоматическая регулировка усиления, дБ.. 50
Размеры, мм..... 28x10x7
Модуль приемника
Входное полное сопротивление ..... более 2 5 кОм (переменный ток), более 3 МОм (постоянный ток)
Ширина полосы звуковых частот, Гц..... 200—8300
Отношение сигнал/шум, дБ..... выше 60
Выходное сопротивление. Ом..... 600 (телефонная линия), 47 (головные телефоны)
Электропитание ..... сеть переменного тока 115/2308,50—60Гц
Размеры, мм..... 265x260x82

**Model SIM-RFM** предназначена для скрытого аудиоконтроля помещения и телефонных линий с использованием имеющихся телефонных сетей. Все разговоры в контролируемых помещениях передаются в дистанционный пункт контроля (мониторинга). В системе применяется техника, не применявшаяся ранее для мониторинга в коммутируемых телефонных системах общего пользования. Система состоит из двух модулей передатчика и приемника частотно-модулированных сигналов. Модуль передатчика содержит высокочувствительный микрофон, предварительный усилитель сигналов микрофона с широким динамическим диапазоном и быстродействующей автоматической регулировкой усиления и частотный модулятор. Модуль защищен от перенапряжений в сети электропитания и телефонных линиях. Модули передатчика выпускаются в различных вариантах, включая версию со скремблером сигналов.

Приемный модуль системы SIM-RFM, заключенный в прочный алюминиевый корпус, рассчитан на прием частотно-модулированных сигналов, содержит преобразователь частоты и усилитель перехваченных сигналов с высоким входным сопротивлением и схемы подавления синфазных сигналов, способствующие получению высокого отношения сигнал/шум. Схемы преобразователя позволяют оператору прослушивать разговоры в помещении и телефонные переговоры одновременно.

Приемный модуль выпускается в версии с дескремблером принимаемых сигналов. Типичный модуль имеет выходы на головные телефоны, магнитофон, переключаемый выход для голосовой активации и сбалансированный выход с сопротивлением 600 Ом для ретрансляции сигналов по линии МККТТ Ml 020 или стандартной линии коммутируемой телефонной сети общего пользования.

**Технические характеристики**

Передатчик RFM
Несущая частота ..... 140 кГц±500 Гц
Выходное полное сопротивление, Ом ... 474
Выходное напряжение, мВ ..... 500
Максимальная девиация
частоты при модуляции, кГц ..... ±5
Ширина полосы звуковых частот, Гц..... 150—3500
Потребляемый ток, мА..... 3 (постоянный ток)
Диапазон регулировки усиления сигналов звуковых частот, дБ..... 50
Размеры (стандартные), мм..... 38x10x10
Приемник RFM
Несущая частота ..... 140 кГц ±500 Гц
Чувствительность, дБ..... -82, при отношении сигнал/шум 20 дБ, -48, при отношении сигнал/шум 50 дБ
Выходное полное сопротивление, кОм... более 1
Ширина полосы звуковых частот, Гц..... 300—5000
Входное полное сопротивление ..... более 25 кОм (переменный ток), более 3 МОм (постоянный ток)
Отношение сигнал/шум, дБ..... более 60
Выходное напряжение, мВ ..... 700 (при отключенной линии), 230 (при выключенном телефоне)
Выходное полное сопротивление ..... 600 Ом (при выключенном телефоне), 1 кОм (при выключенной линии), 47 Ом (при выключенных головных телефонах)

Электропитание ..... сеть переменного тока 115/230 В, 50—60Гц
Размеры, мм..... 265x260x82
Масса, кг..... 2,8

**Model SIM-AWM** — симплексная система аудиомониторинга, обеспечивает высококачественную передачу перехватываемой информации на расстояние до 10 км по неэкранированной двухпроводной линии.

Система стандартной конфигурации содержит миниатюрный передатчик и приемник диапазона очень низких частот (ОНЧ) того или иного типа. Передатчик имеет высокочувствительный микрофон, соединенный с усилителем с широким динамическим диапазоном, быстродействующей автоматической регулировкой усиления, а также модулятор. Передатчик защищен от возможных скачков в системе электропитания. Имеется версия передатчика со скремблированием, защищающим от возможного перехвата третьей стороной или обнаружения работы передатчика методами контрнаблюдения.

**Технические характеристики**

Передатчик
Несущая частота ..... 140кГц± 500Гц
Выходное полное сопротивление. Ом ... 47
Выходное напряжение, мВ ..... 575 (двойная амплитуда)
Девиация частоты при модуляции, кГц... ±5
Ширина полосы звуковых частот, Гц..... 150—3500
Электропитание ..... источник постоянного тока, потребляемый ток 15 мА
Диапазон автоматической регулировки усиления, дБ ..... 50
Размеры, мм..... 24x9x7
Приемник
Несущая частота ..... 140 кГц ± 500Гц
Чувствительность, дБ/мВт..... - 82 при отношении сигнал/шум 20 дБ, -48 при отношении сигнал/шум 50 дБ
Входное полное сопротивление. Ом..... 275
Ширина полосы звуковых частот, Гц..... 300—5000
Выходное напряжение, мВ ..... 700 (при отключенной линии), 230 (при отключенных телефонах)
Выходное полное сопротивление ..... 600 Ом (при отключенном телефоне), 47 Ом (при отключенных головных телефонах)
Электропитание ..... сеть переменного тока, 115/230 В, 50—60Гц
Размеры, мм..... 265x260x82

**Model SIM-SCM** — система аудиомониторинга помещений, передает аудиосигналы по сети электропитания напряжением 220 В. Для передачи используется метод модуляции поднесущей, поэтому несущая, передаваемая по электросети не имеет признаков модуляции. Так как аудиоинформация модулируется дважды, демодуляция на приемной стороне должна осуществляться с последовательным выполнением двух шагов. Передатчик и приемник должны быть согласованы по типу модуляции. Демодуляция сигналов обычным приемником невозможна.

Передатчик включается в сеть так же, как и другие передатчики с сетевым электропитанием. Приемник оформлен в виде отдельного блока с электропитанием от сети. Он имеет регулятор громкости и два выхода: для прослушивания и на магнитофон.

**Технические характеристики**

Передатчик
Частота, МГц ..... 7
Поднесущая, кГц ..... 100—500 (регулируемая)
Ширина полосы звуковых частот, Гц..... 250—5600
Микрофон..... внешний
Электропитание, В..... сеть переменного тока, 220
Размеры, мм..... 30x30x8
Приемник
Выходы ..... на линию и на головные телефоны, с регулировкой громкости
Электропитание, В..... сеть переменного тока, 220
Размеры, мм..... 62x54x84

**Model SIM-ACC** — система аудиоконтроля помещений с передачей информации по проводам электросети SIM-ACC отличается быстротой и простотой установки, что существенно

сокращает время команды по аудио-мониторингу. Стандартная система, включаемая в сеть переменного тока напряжением 110 или 230 В, содержит миниатюрный передатчик, подключаемый к сети параллельно, и приемник частотно-модулированных сигналов диапазона ОНЧ. Для противодействия перехвату передаваемой информации третьей стороной или обнаружения работы передатчика средствами противодействия в передатчике может быть применен скремблер.
Фирма считает, что передатчик системы является самым малогабаритным в мире. Он имеет высокочувствительный микрофон, подсоединенный к усилителю с большим динамическим диапазоном и быстродействующей автоматической регулировкой усиления, а так-

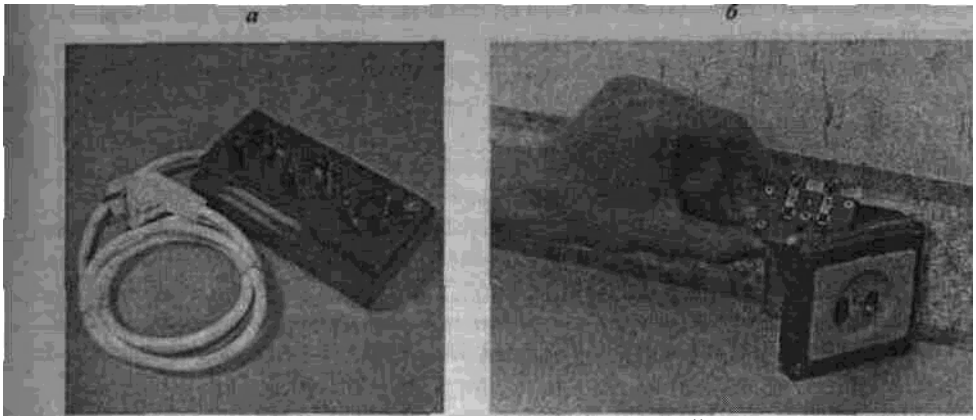


**Рис. 1.3.26. Сетевые закладные устройства, предназначенные для передачи акустической информации по различным сетям:**
а — радиомикрофон в виде электрического тройника; б — радиомикрофон, закамуфлированный под электрическую розетку

же схемы модулятора и защиты от перегрузок в системе электропитания. Блок питания от электросети может иметь разную мощность в зависимости от дальности передачи сигналов.
Приемник содержит входной линейный режекторный («вырезающий» одну частоту) фильтр 50/60 Гц, схемы защиты от перегрузок, малошумящий предварительный усилитель, бесшумную, настройку демодулятор/усилитель звуковых частот с автоматической фазовой подстройкой частоты, параметрический эквалайзер (корректор амплитудно-частотной характеристики) и схемы голосовой активации (VOX).
В приемнике также может быть применен модуль дескремблирования.
Технические характеристики
Передатчик
Несущая частота ..... 140 кГц ± 500Гц
Выходное полное сопротивление, Ом ... 10
Выходная мощность, мВт..... 100
Выходное напряжение..... 500
Девиация частоты при модуляции, кГц... ±5
Ширина полосы звуковых частот, Гц..... 150—3500
Электропитание, мА..... постоянный ток, потребление 3
Диапазон автоматической регулировки усиления звуковых частот, дБ ..... до 66
Размеры, мм..... 24x9x7
Приемник
Несущая частота ..... 140кГц±500Гц
Чувствительность, дБ/мВт..... -82 при отношении сигнал/шум
20 дБ, -48 при отношении сигнал/шум 50 дБ
Входное полное сопротивление, Ом.... 275
Ширина полосы звуковых частот, Гц..... 300—500
Выходное полное сопротивление ..... 1 кОм (при отключенной линии),
600 Ом (при отключенном телефоне), 47 Ом (при отключенных головных телефонах)
Электропитание ..... сеть переменного тока, 115/230 В, 50—60Гц
**Размеры, мм**..... 265x255x88
Внешний вид некоторых закамуфлированных ЗУ, предназначенных для установки в сетях электропитания 220В, показаны на рис. 1.3.26.

### 1.3.3. Направленные микрофоны

**Общие понятия о направленных микрофонах**

В начале 90-х годов направленные микрофоны вызывали повышенный интерес у организаций и частных лиц, которые занимались вопросами сбора информации с помощью технических средств. Это было связано с тем, что очень немногие люди ранее имели дело с данной техникой, а различные буклеты отечественных и зарубежных фирм рекламировали «универсальное средство получения информации». В технических описаниях приводились фантастические данные о дальности съема информации (до 2000 м) и коэффициентах направленного действия (до 50 дБ) при достаточно скромных габаритах (не более полуметра) и относительно невысокой стоимости (50... 800 $). Под впечатлением от таких характеристик у потенциальных клиентов в голове возникали планы безопасного и простого перехвата речевой информации с помощью замечательного направленного микрофона.

В то же время многие стали опасаться, что их переговоры будут «считываться со стекол окон офисов, квартир и автомобилей», да и на улице теперь любые встречи не представлялись конфиденциальными. Разжиганию страстей способствовали «шпионские» фильмы, научно-популярные статьи в различных изданиях, выступления «специалистов с большим практическим стажем работы со спецтехникой».

В результате, в 1991—1994 годах в России наблюдался массовый спрос на направленные микрофоны. Их приобретали как вновь образованные спецслужбы, получившие право на оперативно-розыскную деятельность, так и частные службы безопасности, детективные агентства, бандиты и авантюристы всех мастей. Однако результаты попыток применения микрофонов обескураживали. О километрах никто уже не вспоминал, да и прослушивание разговора на расстоянии в 100 м получалось крайне редко. Раздосадованные покупатели обвиняли фирмы в том, что им «подсунули некачественный товар», а продавцы, в свою очередь, ссылались на неумение применять технику на практике. Следствием этого стало резкое падение интереса к направленным микрофонам со стороны всех потенциально заинтересованных в добывании информации лиц. Соответственно, необходимостью защиты информации в случае возможного применения данной техники начали пренебрегать, хотя в 1995—1996 годах на рынке России были представлены около двух десятков типов направленных микрофонов как отечественного, так и иностранного производства. Сотни единиц оказались в руках далеко не самых законопослушных граждан.

Для того чтобы оценить возможности направленных микрофонов и степень опасности, которую они могут представлять в руках недобросовестных конкурентов, необходимо понять используемые в приборах физические принципы. Ибо без этих знаний невозможно организовать успешную защиту своих секретов от подобных преступных посягательств.

В наиболее общем виде любой направленный микрофон можно представить как некоторый комплекс, состоящий из чувствительного элемента (собственно микрофона), осуществляющего акустико-электрическое преобразование, и механической системы (акустической антенны), обеспечивающей направленные свойства комплекса.

**Микрофон**

Микрофон (от греч. mikros — малый и phone — звук) — это электроакустический прибор для преобразования звуковых колебаний в электрические.

В зависимости от принципа действия микрофоны делят на следующие типы:

**>-** порошковые угольные;
>- электродинамические;
>- электростатические (конденсаторные и электретные);
>- полупроводниковые;
**>-** пьезоэлектрические;
>- электромагнитные.

Порошковый угольный микрофон впервые был сконструирован русским изобретателем М. Махальским в 1878 году и позже, независимо от него, П. М. Голубицким в 1883-м. Принцип действия такого микрофона основан на том, что угольная или металлическая мембрана под действием звуковых волн колеблется, изменяя плотность и, следовательно, электрическое сопротивление угольного порошка, находящегося в капсюле и прилегающего к мембране. Вследствие неравномерного механического давления сила тока, протекающего через микрофон, изменяется в акустический сигнал. Однако в интересах съема информации микрофоны данного типа практически не используются из-за

их низкой чувствительности и большой неравномерности амплитудно-частотной характеристики.
Электродинамический микрофон катушечного типа изобрели американские ученые Э. Венте и А. Терас в 1931 году. В нем применена диафрагма из полистирольной пленки или алюминиевой фольги. Катушка, сделанная из тонкой проволоки, жестко связана с диафрагмой и постоянно находится в кольцевом зазоре магнитной системы. При колебаниях диафрагмы под действием звуковой волны витки катушки пересекают магнитные силовые линии и в обмотке наводится электродвижущая сила (ЭДС), создающая переменное напряжение на выходе микрофона. Вместо катушки может использоваться ленточка из очень тонкой (около 2 мкм) металлической фольги.
В конденсаторном микрофоне, изобретенном американским ученым Э. Венте в 1917 году, звуковые волны действуют на тонкую металлическую мембрану, изменяя расстояние и, следовательно, электрическую емкость между мембраной и металлическим неподвижным корпусом, которые представляют собой пластины электрического конденсатора. При подведении к пластинам постоянного напряжения изменение емкости вызывает появление тока через конденсатор, сила которого изменяется в такт с колебаниями звуковых частот.
Электретный микрофон, изобретенный японским ученым Егути в начале 20-х годов XX века, по принципу действия и конструкции схож с конденсаторным. Только роль неподвижной обкладки конденсатора и источника постоянного напряжения в нем играет пластина из электрета. Недостатком такого микрофона является высокое выходное сопротивление, которое приводит к большим потерям сигнала, поэтому в корпус элемента, как правило, встраивают истоковый повторитель, что позволяет снизить выходное сопротивление до величины не более 3...4 кОм.
В пьезоэлектрическом микрофоне, впервые сконструированном советскими учеными С. Н. Ржевкиным и А. И. Яковлевым в 1925 году, звуковые волны воздействуют на пластинку из вещества, обладающего пьезоэлектрическими свойствами (например, из сегнетовой соли), вызывая на ее поверхности появление электрических зарядов.
В электромагнитном микрофоне звуковые волны воздействуют на мембрану, жестко связанную со стальным якорем, находящимся в зазоре обмотка неподвижной катушки. В результате воздействия акустических волн на такую систему на выводах обмотки появляется ЭДС. Данные изделия так же, как и порошковые угольные микрофоны, не получили широкого распространения из-за большой неравномерности амплитудно-частотной характеристики.
Обобщенные характеристики перечисленных типов микрофонов приведены в табл. 1.3.4.

**Таблица 1.3.4. Основные характеристики акустических приемников-микрофонов**

Тип микрофона /Диапазон частотной характеристики, Гц /Неравномерность воспроизводимых частот, дБ /Осевая чувствительность на частоте 1кГц, мВм$^2$/н
Порошковые угольные /300...3400 /20 /1000
Электродинамические /30...15 000 /12 /1
Конденсаторные /30...15 000 /5 /5
Электретные /20...18 000 /2 /1
Пьезоэлектрические /100...5000 /15 /50
Электромагнитные /300... 5000 /20 /5

Чаще всего в направленных микрофонах применяются чувствительные элементы (микрофоны) электретного типа, так как они имеют наилучшие электроакустические характеристики: широкий частотный диапазон; малую неравномерность амплитудно-частотной характеристики; низкий уровень искажений, вызванных нелинейными и переходными процессами, а также высокую чувствительность и малый уровень собственных шумов.
Точность воспроизведения перехватываемых акустических сигналов (разборчивость речи) зависит не только от типа микрофона. Важное значение имеют и характеристики электронного блока, состоящего из микрофонного усилителя и головных телефонов. В большинстве же случаев, из экономических соображений фирмы, поставляющие направленные микрофоны, комплектуют их дешевыми электронными блоками, соответствующими аппаратуре 3-го класса бытовой техники. Поэтому владельцы таких средств зачастую вынуждены сами подбирать акустический усилитель и головные телефоны с требуемыми параметрами.
Однако самое главное в направленных микрофонах — это свойства его акустической

антенны.

**Акустические антенны** являются именно теми основополагающими элементами, которые определяют облик и основные характеристики комплексов дистанционного перехвата речевой информации. Назначение их заключается в усилении звуков, приходящих по основному направлению, и существенном ослаблении всех остальных акустических сигналов.

В настоящее время разработано несколько модификаций антенн, в соответствии с которыми существует следующая классификация направленных микрофонов (рис. 1.3.27):

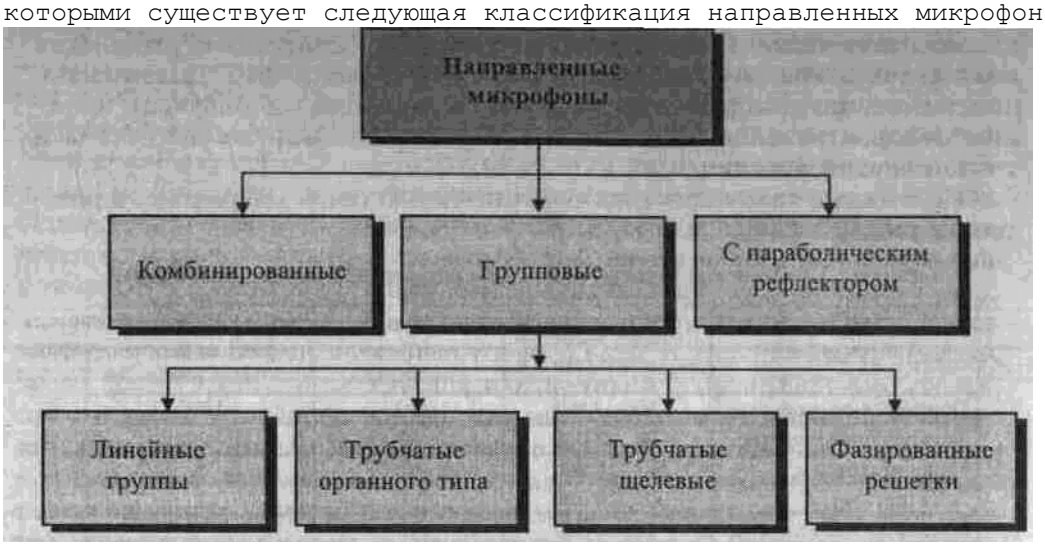



**Рис. 1.3.27. Классификация направленных микрофонов**

**>-** комбинированные;
**>-** групповые, в том числе:
**>-** линейные группы микрофонов;
**>-** трубчатые приемники органного типа;
**>-** трубчатые щелевые приемники;
>- фазированные решетки;
**>-** микрофоны с параболическим рефлектором.

Для сравнительной оценки качества вышеперечисленных направленных микрофонов используют технические характеристики, основными из которых являются характеристика направленности и индекс направленности.

Характеристика, или диаграмма, направленности — это чувствительность микрофона в зависимости от угла q между рабочей осью микрофона и направлением на источник звука. Ее определяют или на ряде частот, или в пределах полосы частот. Обычно используют нормированную характеристику направленности R(Q), то есть зависимость отношения чувствительности $E_\theta$ измеренной под углом q, к осевой (максимальной) чувствительности Eос.

$R(\theta)=E_\theta/E_{oc}$

Большинство микрофонов имеет осевую симметрию, поэтому характеристика направленности для них одинакова во всех плоскостях, проходящих через ось микрофона. Графическое представление характеристик направленности часто дают в полярных координатах (рис. 1.3.28).

Индекс направленности показывает выраженную в децибелах разницу уровней мощности сигналов на выходе микрофона от двух источников звука: одного (например, голоса человека), расположенного на оси, и другого — источника рассеянных звуковых волн (например, шума автотрассы), если оба создают в точке расположения микрофона одинаковое акустическое давление. Иными словами, индекс направленности показывает величину подавления (дискриминации) шума, приходящего с бокового направления, по отношению к сигналу, приходящему с направления, совпадающего с осью микрофона.

Ненаправленный микрофон не подавляет шума, поэтому его индекс направленности равен нулю (Qнм = 0 дБ).

Коэффициент направленного действия показывает выраженную в децибелах степень увеличения уровня сигнала на выходе микрофона при замене ненаправленного микрофона направленным и постоянной величине акустического давления.

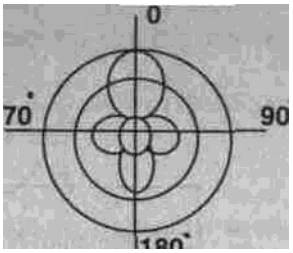



**Рис. 1.3.28. Характеристика направленности микрофона**

**Комбинированные микрофоны**

Эти устройства являются простейшим видом направленных микрофонов, так как представляют из себя систему, состоящую из двух типов акустических приемников-микрофонов. Обычно это приемники давления и градиента давления, реагирующие соответственно на величину и изменение величины акустического сигнала.

Простейшая комбинация этих приемников, наиболее часто применяемая на практике, состоит из одного микрофона-приемника давления и одного микрофона-приемника градиента давления, располагаемых как можно ближе друг к другу (обычно один над другим) и так, чтобы их оси были параллельны.

Изменяя параметры микрофонов, можно получать различные характеристики направленности и соответственно индексы направленности (рис. 1.3.29) всей системы. Наибольший индекс достигается для случая, когда диаграмма имеет вид гиперкардиоиды (Qгк = 6 дБ).

**Групповые микрофоны**

В соответствии с классификацией, приведенной на рис. 1.3.27, к групповым акустическим приемникам относятся линейные группы, трубчатые 1 микрофоны и фазированные решетки.

Рассмотрим их более подробно.

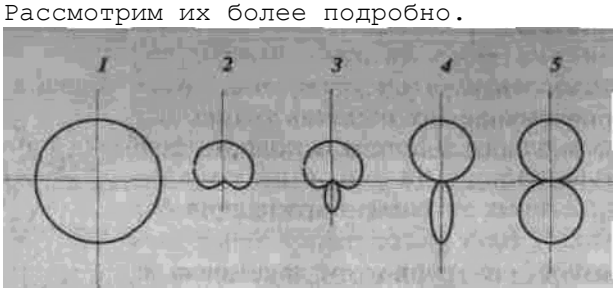



**Рис. 1.3.29. Виды характеристик направленности для комбинированных микрофонов:**

1 — окружность для приемника давления; 2 — кардиоида для комбинированного приемника с одинаковой чувствительностью приемников давления и градиента давления; 3 — суперкардиоида; 4 — гиперкардиоида; 5 — косинусоида (восьмерка) для одного приемника градиента давления

Линейная группа приемников (микрофонов) — это несколько микрофонов, обычно располагаемых в ряд по прямой горизонтальной линии так, чтобы их оси были параллельны друг другу (рис. 1.3.30), иногда микрофоны располагают по небольшой дуге. Электрические выходы акустических приемников последовательно соединяют в специальном смесителе.

Характеристика направленности такой линейной группы R(Q) из N элементов определяется как произведение характеристики направленности одиночного приемника $R_1(\theta)$ на характеристику группы:

$R(\theta)=R_1(\theta)[\sin Nx /(N\sin x)]$,

где x = p (d/l) sin q, a d — расстояние между отдельными приемниками.

Чем меньше отношение длины волны l акустического сигнала к длине группы l = (N - 1)/d, тем уже будет основной лепесток диаграммы направленности и больше индекс направленности. Однако следует иметь в виду, что при чрезмерной длине группы (сравнимой с расстоянием от приемника до источника звука) будут сказываться интерференционные явления из-

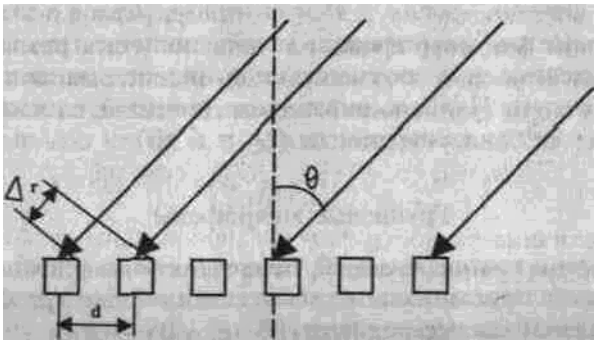



**Рис. 1.3.30. Общий вид линейной группы микрофонов**

за большой разности хода звуковых волн от источника до входов отдельных микрофонов, входящих в состав группы.

Численное значение ширины основного лепестка определяется из соотношения:

$$\theta_1 = \arcsin(\lambda/l).$$

Так, например, для группового приемника, состоящего из шести ненаправленных микрофонов, расположенных по прямой линии с шагом d= 10 см (l = 50 см) и частотой принимаемого сигнала f = 1000 Гц (λ = 33 см), ширина основного лепестка составляет величину $\theta_1$ = 41°. Расчет индекса направленности для этой группы дает величину 8 дБ.

Основной недостаток такого типа направленных микрофонов — это обеспечение направленных свойств только в плоскости, проходящей через оси микрофонов; в ортогональной плоскости характеристика такая же, как и у одиночного микрофона.

Трубчатый микрофон органного типа так же использует свойства групповых антенн. Его вид схематично представлен на рис. 1.3.31.

Такой микрофон имеет в своем составе несколько десятков тонких трубок 1 с длинами от нескольких сантиметров до метра и более. Эти трубки собирают в пучок — длинные по середине, короткие — по наружной поверхности. Концы трубок с одной стороны образуют плоский срез 2, входящий в предкапсюльный объем 4. Сам микрофонный капсюль 3 выбирается, как правило, электродинамического или электромагнитного типа (приемника давления) в зависимости от требуемого частотного диапазона. Звуковые волны, приходящие к приемнику по осевому направлению, проходят в трубки и поступают в предкапсюльный объем в одинаковой фазе. Их амплитуды складываются арифметически:

$$U_\Sigma = \sum_{i=1}^{N} U_i,$$

где N — количество трубок, а U — амплитуды звуковых волн. Звуковые волны фонового шума, приходящие под углом 6 к оси, оказываются сдвинутыми по фазе, так как трубки имеют разную длину, поэтому

амплитуды этих волн складываются геометрически:

$$U_\Sigma = U_i^2 + U_{i+1}^2 - 2U_iU_{i+1}\cos\Delta\varphi,$$

где Дф — величина разности фаз для любой пары звуковых волн, при->. шедших по трубкам, длины которых отличаются на величину d:

$$\Delta\varphi = \pi(d/\lambda)(1-\cos\theta).$$

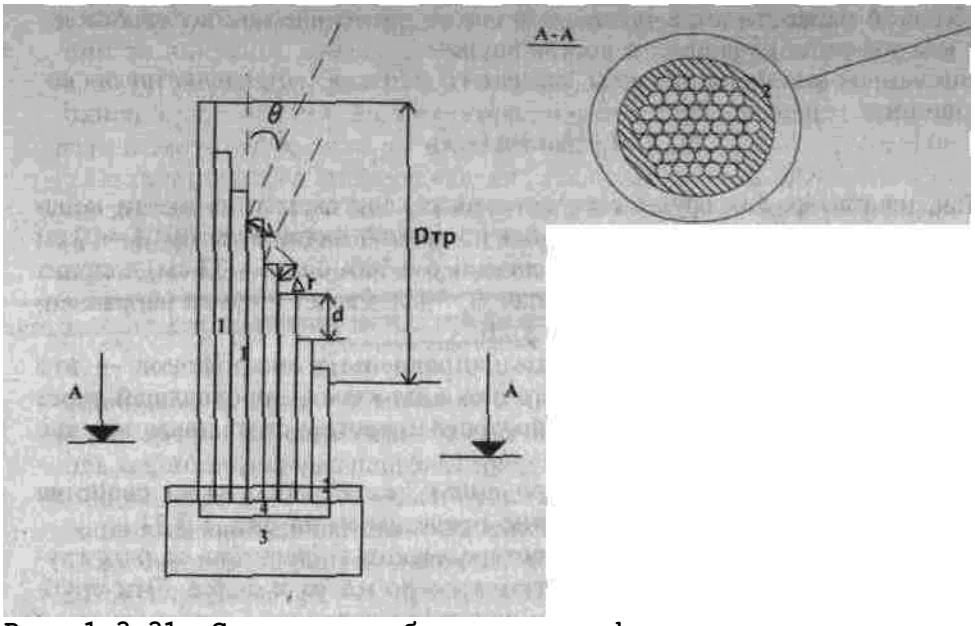



**Рис. 1.3.31. Строение трубчатого микрофона органного типа:**
1 — звуковые трубки; 2 — срез трубок; 3 — капсюль микрофона; 4 — предкапсюльный объем

Характеристика направленности для такого направленного микрофона определяется из соотношения, аналогичного для линейной группы приемников:

$R(\theta)=\sin Nx / (N \sin x)$,

где $x = \pi (d_{min}/\lambda)(1-\cos \theta)$, $d_{min}$ — разница в длине между ближайшими по размеру трубками.

Приведенные соображения справедливы в случае, если в трубке не образуются резонансные колебания. С этой целью входные отверстия трубок либо их концы у капсюля закрывают при помощи пробок из пористого поглотителя.

Основным достоинством таких направленных микрофонов является высокий индекс направленности (около 8 дБ, при этом шумы, действующие с боковых направлений, ослабляются по отношению к сигналу почти в 10 раз). Основной недостаток — довольно большие геометрические размеры (максимальная длина трубок около 90 см).

На сегодняшний день подобные устройства практически не используются, за исключением нескольких экспериментальных изделий.

Трубчатый щелевой приемник (иногда его называют приемником бегущей волны) — представляет собой трубку с отверстиями или сплошной осевой прорезью по всей длине. С некоторым приближением такую трубку можно рассматривать как множество трубок разной длины, поэтому трубчатый щелевой микрофон и относят к приемникам группового типа.

Если звук приходит по оси, то пути его распространения по трубке и через отверстия одинаковы и составляющие звукового давления от пришедших колебаний синфазны и, следовательно, сумма их, воздействующая на диафрагму микрофонного капсюля, максимальна. Если же звук приходит под углом q v. оси трубки, то разность пути звука по всей трубке и пути от входа в трубку до входа в отверстие, находящееся на расстоянии d, обусловит сдвиг фаз, определяемый как $\Delta\varphi = 2\pi d\,(1-\cos\theta)/\lambda$. В свою очередь, это создает сдвиг фаз различной величины между колебаниями, пришедшими через разные отверстия, что приводит, как и в предыдущем случае, к уменьшению результирующего давления на диафрагму.

Следует отметить, что чем более высокую направленность требуется получить, тем больше должна быть длина звукоприемного элемента (трубки), так как индекс направленности увеличивается с увеличением отношения длины трубки к длине волны принимаемого излучения. Для того чтобы не образовывалось стоячих волн, наружный конец звукоприемного элемента (трубки) закрывают поглощающей тканью.

Данный тип направленного микрофона получил наибольшее распространение. Причин этому можно назвать несколько:

>- простота изготовления и, как следствие, низкая стоимость;

>- наличие в стране нескольких производителей данной техники;
>- простота в применении;
>- возможность организации различных вариантов камуфляжа.

Рассмотрим в качестве примера несколько типов направленных микрофонов трубчатого щелевого типа.

Отечественный остронаправленный микрофон **МД-74** состоит из собственно микрофона динамического типа и примыкающей к нему трубки длиной 0,8 м. В стенках трубки (рис. 1.3.32) проделан ряд отверстий через равные промежутки. Для компенсации падения чувствительности микрофона на высших частотах из-за большого поглощения их в трубке вокруг каждого из отверстий устанавливаются концентраторы — рупорки. Размеры их подобраны таким образом, чтобы обеспечить подъем частотной характеристики на высших частотах диапазона до 10...12 дБ. Основные параметры микрофона приведены в табл. 1.3.5.

В другом направленном микрофоне трубчатого типа **КМС-19-05** рупорки отсутствуют. Он предназначен для профессиональной записи звука при работе на относительно больших расстояниях от источника (до 100 м), в условиях повышенного окружающего шума. Основные его параметры также приведены в таблице. Блок усиления на ремнях размещается на боку оператора, что создает определенное удобство в работе. Однако опыт работы с такими микрофонами показывает, что декларируемые 100 м дальности возможно получить только в тихой загородной местности. В относительно

**Таблица 1.3.5. Основные характеристики некоторых трубчатых щелевых направленных микрофонов**

Тип микрофона /Номинальный диапазон частот, Гц /Неравномерность частотной характеристики, ДБ /Чувствительность холостого хода на частоте 1000 Гц, мВ/Па /Направленные свойства /Внешние размеры, мм /Масса, кг

МД-74 /10...10000 /8 /1,2 /Остронаправленный (индекс направленности на частотах выше 125 Гц -не менее 6 дБ /071х810 /0,5

КМС-19-05 /20...20 000 /8 /45 /Остронаправленный /024х850 /0,28

КМС-1909 /20...20 000 /8 /30 /Односторонне направленный (угол раскрытия 115° при спаде на 6 дБ) /024х203 /0,19

МКЕ-802 /50.., 15 000 /7 /13 /Суперкардиоида /022х292 /0,185

тихом городском дворе — порядка 30 м, а на достаточно оживленной улице — 10...15 м. Можно предполагать, что подобные дальности присущи всем направленным микрофонам данного типа как отечественного, так и иностранного производства.

Следует отметить, что многие направленные микрофоны трубчатого типа комплектуются ветрозащитным чехлом, обычно из поролона, благодаря чему снижается чувствительность к помехам от ветровых атмосферных воздействий.

К базированным решеткам можно отнести все описанные выше устройства, но по устоявшейся в настоящее время терминологии к ним относят изделия, имеющие плоскость, на которой расположены открытые торцы звуководов; они обеспечивают синфазное сложение звуковых полей от источника в некотором акустическом сумматоре, на выходе которого расположен микрофон (рис. 1.3.33). Если звук приходит с осевого направления, то все сигналы, распространяющиеся по звуководам, будут в фазе, и сложение в акустическом сумматоре даст максимальный результат. Если направление на источник звука не осевое, а под некоторым углом к оси, то сигналы от различных точек приемной плоскости будут разными по фазе и результат их сложения будет меньше; При этом число приемных точек может достигать нескольких десятков. Очевидно, что подобная решетка

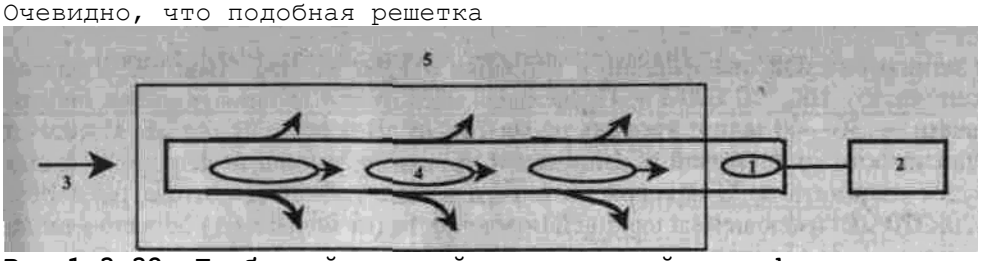



**Рис.1.3.32. Трубчатый щелевой направленный микрофон:**

1 — микрофон; 2 — усилитель; 3 — звуковые волны; 4 — щели; 5 — ветрозащитный поролоновый чехол

является менее громоздкой, чем микрофон органного типа, но она существенно проигрывает последнему в направленных свойствах.

Коэффициент направленного действия для данного типа направленного микрофона можно приблизительно определить по формуле:

$$Q = 4\pi S/\lambda^2 = 4\pi N^2(0{,}5\lambda^2)/\lambda^2 = \pi N^2,$$

где S — площадь входной аппертуры, м$^2$; λ — длина волны звука, м; N— число элементов решетки.

Надо отметить, что данная формула применима при расположении элементов антенной решетки по фронту на расстоянии около 15 см.

Примером направленного микрофона такого типа является изделие **«Шорох».** Оно относится к устройствам, предназначенным для прослушивания

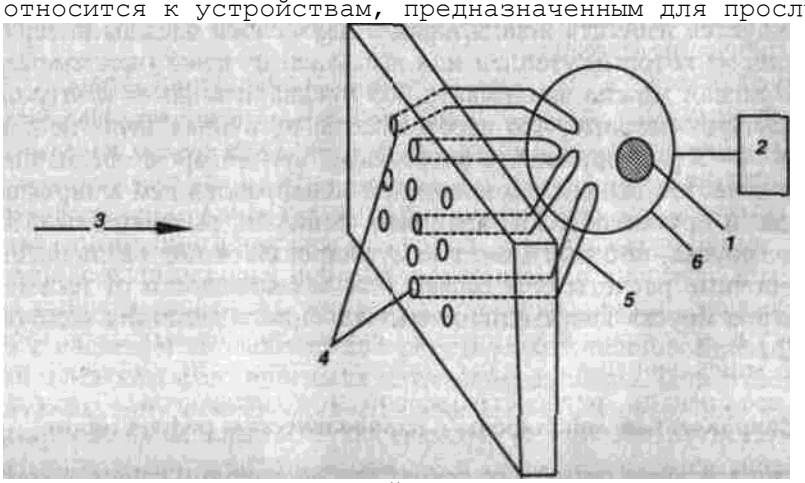



**Рис. 1.3.33. Направленный микрофон типа «фазированиая решетка»:**

1 — микрофон; 2 — усилитель; 3 — звуковая волна; 4 — торцы звуководов;

5 — звуководы; 6 — акустический микрофон

и записи речевой информации в условиях открытого пространства, в диапазоне частот 100...10 000 Гц. Предельная паспортная дальность съема информации — 30—40 м при уровнях шума 74...76 дБ и речи 70...74 дБ. Однако в зависимости от шумовой обстановки и уровня информации дальность съема будет изменяться. Микрофон выполнен в виде гибкой пластины размером 320х320 мм, имеющей на внешней поверхности (от оператора) большое число акустических входных отверстий. За счет звуководов и суммирующих устройств образуется фазированная решетка, позволяющая сформировать диаграмму с шириной основного лепестка около 30...40° на частоте 1 кГц. Коэффициент направленного действия составляет около 12 дБ.

Микрофон, размещенный в специальном чехле, может устанавливаться на теле оператора, под одеждой в варианте грудь—спина (фронт—тыл). На поясе чехла размещен манипулятор, состоящий из усилителя низкой частоты с автоматической регулировкой усиления, источника питания и органов управления: включено—выключено с первоначальной установкой уровня полезного сигнала и два выхода на магнитофон и головные телефоны. Функциональные возможности изделия могут расширяться за счет дополнительной установки радиоканала и других сервисных устройств. Конструктивные особенности позволяют легко камуфлировать микрофон под папку, дипломат, картину и т. д.

Так как работа в помещении характеризуется наличием большого количества переотраженных сигналов от различных элементов строительных конструкций в виде стен, потолков, колонн, то максимальная эффективность работы такого направленного микрофона достигается в помещениях с объемом более 500 м$^3$.

Рекомендуется избегать использования двух слоев одежды поверх микрофона, один из которых утеплен или выполнен из кожи (кожзаменителя). Полезный сигнал можно записывать без предварительного контроля, но при этом следует помнить, что расстояние до источника звука не должно, более, чем 4—5 раз, превышать расстояние, при котором обеспечивается требуемое качество записи, выполненной ненаправленным

микрофоном.
Известны и другие образцы антенных решеток, выполненные, например, в виде бруска, который может камуфлироваться под различные предметы. Оценочные расчеты показывают, что в зависимости от геометрических размеров бруска коэффициент направленного действия находится в пределах 2...5 дБ.

**Направленные микрофоны с параболическим рефлектором**

Принцип действия подобных устройств достаточно прост и понятен. Микрофон размещен в фокусе отражателя параболической формы (рис. 1.3.34). Звуковые волны с осевого направления, отражаясь от параболического зеркала, суммируются в фазе в фокальной точке. Возникает усиле-

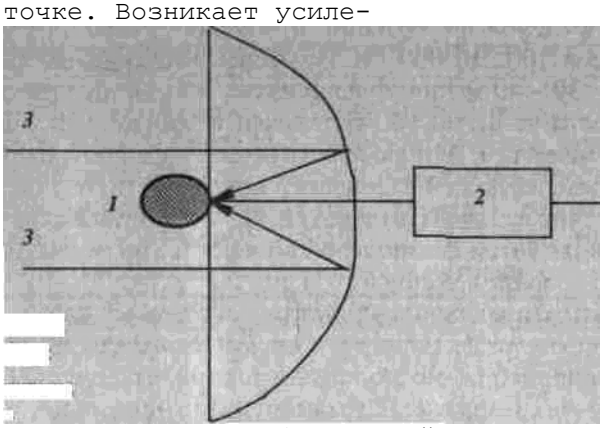



**Рис. 1.3.34. Параболический направленный микрофон:**
1 — микрофон; 2 — усилитель; 3 — звуковая волна

ние звукового поля. Чем больше диаметр зеркала, тем большее усиление может обеспечить устройство. Если направление прихода звука не осевое, то сложение отраженных от различных частей параболического зеркала звуковых волн, приходящих в фокус, даст меньший результат, поскольку не все слагаемые будут в фазе. Ослабление тем сильнее, чем больше угол прихода звука по отношению к оси. Создается, таким образом, угловая избирательность по приему.
Коэффициент направленного действия для данного типа направленного микрофона можно приблизительно определить по формуле:

$$Q = 4\pi S_э/\lambda^2,$$

где Sэ — эффективная поверхность антенны.
Понятие эффективной поверхности тесно связано с максимальной мощностью, которая может быть извлечена приемной антенной из падающей плоской акустической волны. При выполнении ряда условий (D > 1, где D — диаметр рефлектора; совмещение максимума диаграммы направленности с направлением прихода волны и т. д.) можно приближенно считать, что Sэ≈S, где S — площадь входной аппертуры, м$^2$.
Как правило, фирмами-изготовителями поставляется в комплекте блок усиления с системой автоматической регулировки усиления и выходами на наушники и магнитофон, иногда акустические фильтры. При работе параболическую антенну с микрофоном можно держать в руках или закрепить на треноге.
В качестве примеров направленных микрофонов с параболическим отражателем рассмотрим несколько систем. Портативный параболический приемник **PRO-200** предназначен для дистанционного приема звуковых волн. Обладает высокой чувствительностью и острой диаграммой направленности параболического зеркала. Оборудован дополнительным регулируемым фильтром, позволяющим осуществлять частотную селекцию сигнала по ширине и положению его спектра на оси частот. Паспортная дальность — 1 км (?). Очевидно, что в рекламных целях она приведена для наилучших условий приема: тихая открытая местность, ночь, человек говорит в полный голос. Имеется возможность подключения к магнитофону. Питание — от встроенного аккумулятора или внешнего зарядного устройства от сети 220 В. Диаметр зеркала — 60 и 75 см (качество приема улучшается с увеличением диаметра).
Значения коэффициента направленного действия (КНД) антенны в зависимости от диаметра зеркала и частоты принимаемого акустического сигнала приведены в табл. 1.3.6.

**Таблица 1.3.6. Значения коэффициента направленного действия антенны в зависимости от диаметра зеркала и частоты принимаемого акустического сигнала**

Частота, Гц /КНД при диаметре зеркала 0,6 м /КНД при диаметре зеркала 0,75 м
500 /1 /11
1000 /15 /17
5000 /19 /31
10000 /35 /37

Другой направленный микрофон (типа А—2) имеет параболический отражатель диаметром 43 см, снабжен усилителем и наушниками. Паспортная дальность действия на открытой местности также заявлена около 1 км (!). Коэффициент усиления электронного блока — не менее 80 дБ. Имеется система автоматической регулировки усиления с динамическим диапазоном входных сигналов 40 дБ. Питание от стандартной батарейки 9 В. Предусмотрен разъем для подключения магнитофона.

Параболические направленные микрофоны РК375 и РК390 (производство Германии) имеют следующие параметры.

**РК375:** габариты — 0600х300 мм, масса — 1,2 кг, коэффициент усиления — 90 дБ, питание — 5В, автономность — 75 часов.

РК390, соответственно: 0130х100 мм, 1,1 кг, 70 дБ, 9 В, 50 часов. Паспортная дальность — до 50 м (пунктуальности немцев можно позавидовать).

Особенности оперативного применения направленных микрофонов таковы, что неподготовленный человек не сможет их скрытно использовать, так как необходимо не только правильно расположиться относительно объекта разведки и источников шумов, но при этом и самому не быть обна-


**Рис. 1.3.35. Направленные микрофоны для дистанционной записи перехватываемой акустической информации:**

а — параболический; б — трубчатый щелевой

руженным. Последнее практически невозможно в случае использования направленных микрофонов с параболическими отражателями из-за их существенных размеров.

Зарубежные специалисты рекомендуют применять такие микрофоны только в условиях ограниченной видимости и при относительно низких уровнях окружающих шумов — ночью, в парках, сельской местности и т. п. При этом честно информируют, что акустический телескоп может не улавливать звуки на большом (заявленном) расстоянии, если он используется недалеко от автомагистралей или в местах с повышенным уровнем фонового шума.

Поэтому подобные системы редко применяются для съема информации. Их используют в основном журналисты, ученые, кинематографисты и т. д. Даже в рекламных проспектах производителей спецтехники указывается, что подобные микрофоны незаменимы при спортивных соревнованиях, охоте, экскурсиях на природе, для двусторонней дискретной связи.

Внешний вид некоторых типов направленных микрофонов представлен на рис. 1.3.35.

**Перспективы развития направленных микрофонов**

Конструкция направленных микрофонов непрерывно совершенствуется, так как проблема дистанционной записи речи становится все более актуальной в рамках развития систем

негласного съема информации. Однако революционного переворота (в смысле увеличения радиуса перехвата до километров) в данной области техники не предвидится. В то же время можно выделить следующие направления улучшения характеристик направленных микрофонов:

1. Возможно появление приборов, способных к адаптивной пространственно-временной фильтрации акустических помех. Объективной основой таких приборов являются достижения в области цифровой многоканальной обработки данных (специализированный компьютер станет такой же привычной составной частью направленного микрофона, как наушники);
2. Прогресс в области высокочувствительных акустических сенсоров принципиально позволяет в ближайшем будущем создать микрофоны с пороговой чувствительностью -10...-15 дБ, что позволит несколько повысить дальность перехвата акустической информации (при отсутствии акустических помех и шумов);
3. Возможно появление принципиально новых устройств, использующих нелинейные и параметрические эффекты для реализации органолептических скрытых антенн большого размера, способных увеличить коэффициент направленного действия до 25 дБ и более.

**Особенности применения направленных микрофонов**

Так как на дальность ведения разведки влияют не только параметры микрофонов, но и условия, в которых применяются эти устройства, следует знать некоторые особенности использования направленных микрофонов.

НА ОТКРЫТОЙ МЕСТНОСТИ

К открытой местности обычно относят участки, не имеющие ярко выраженных ограждающих конструкций, которые создают замкнутый объем.

Как правило, это улицы, площади, стадионы, дворы, парки, залы летних. кафе, пляжи и т. п. К работе на открытых площадках относят и прослушивание разговоров, ведущихся в помещениях, если перехват ведется через открытое окно, форточку или опущенное стекло автомобиля.

Основными ограничениями на ведение негласного съема информации в таких условиях является затухание, которое испытывает сигнал при его распространении, и высокий уровень фоновых шумов.

Величина затухания обусловливается рядом факторов, которые зависят как от характеристик самого звука, так и от свойств среды распространения. Все их делят на две большие группы.

В первую входят факторы, связанные с законами распространения акустических волн. А именно:

>- при распространении в неограниченной среде от источника конечных размеров интенсивность звука убывает обратно пропорционально квадрату пройденного расстояния;

>- неоднородности среды (капли дождя, ветки деревьев и другие препятствия) вызывают рассеяние звуковых волн, приводящее к ослаблению сигнала в «основном» направлении;

>- на распространение звука в атмосфере влияют турбулентности, распределения температуры и давления, сила и скорость ветра, которые вызывают искривление звуковых лучей, а иногда вообще нарушают передачу звука.

Действительно, звуковая волна, попадая на границу раздела двух слоев атмосферы с различными характеристиками, частично отражается, а частично проникает в другой слой. При этом преломление волны происходит в соответствии с законом физики, гласящим, что отношение угла падения к углу преломления (определяется отношением скоростей распространения звуковых колебаний в этих средах (слоях):

$\sin\varphi_1/\sin\varphi_2=C1/C2$

где С1, и С2 — скорости звука в обеих средах.

Если параметры обоих слоев близки друг к другу, то фактически вся энергия переходит из одной среды в другую и $\varphi_1\approx\varphi_2$. Когда же параметры различны, имеет место искривление звуковых лучей.

Именно по этой причине оператор часто вынужден размещать микрофон как можно выше над поверхностью земли, чтобы обеспечить максимальную дальность перехвата акустических сигналов.

Вторая группа связана с физическими процессами в веществе — необратимыми переходами звуковой энергии в другие формы (главным образом в тепло). Можно выделить следующие факторы, определяющие степень поглощения звуковых волн:

>- поглощение звука возрастает пропорционально квадрату частоты (поэтому колебания с частотами выше 1000 Гц затухают особенно быстро);
>- степень поглощения растет при уменьшении относительной влажности воздуха (так, например, при влажности 50 % акустические сигналы с частотой 10 кГц затухают только на 14 дБ на каждые 100 м, а при уменьшении влажности до 15 % затухание возрастает вдвое и достигает 28 дБ; ветер, дождь и снег могут добавить еще 8...10 дБ на каждые 100 м).

Строго говоря, открытых пространств, в которых звуковые волны распространялись бы беспрепятственно во всех направлениях, практически нет, так как всегда имеют место отражения от земной поверхности, стен ближайших зданий, предметов и т. п. Однако эти переотражения можно учесть, а иногда и просто пренебречь ими, если они незначительны из-за высокого коэффициента поглощения (например, от снежного покрова).

Высокий уровень акустических шумов — другая специфика открытых пространств.

Для осуществления оценки влияния их на качество фиксации акустической информации используют понятие уровня громкости, под которым понимают уровень равногромкого с мешающим сигналом чистого тона на частоте 1000 Гц, выраженный в децибелах. За единицу уровня принимают 1 (один) Фон, то есть:

$Lg[Фон]=L_{1000Гц}[Дб]$.

В табл. 1.3.7 приведены уровни громкости различных шумов в зависимости от дальности источника. Сравнивая приведенные значения с уровнем обычной речи, который составляет 65... 75 дБ, делают вывод о степени влияния акустических помех на качество перехвата.

Некоторые предельные дальности регистрации приведены в табл. 1.3.8.

Из вышесказанного следует, что на дальность фиксации речевой информации на открытом участке местности влияют следующие факторы: направление и сила ветра, температура и влажность воздуха, характер рельефа, наличие строений, растительность, уровни фоновых шумов. Дальность ведения разведки увеличивается, если ветер дует со стороны источника звука, ночью и ранним утром, в пасмурную погоду, особенно после дождя, у водной поверхности, в горах, зимой (при отсутствии снегопада). Звук поглощается (становится слабее) в жаркую солнечную погоду, во время снегопада, дождя, в лесу, кустарнике и на местности с песчаным грунтом, при наличии искусственных и естественных препятствий.

Следует еще раз подчеркнуть, что приведенные цифры относятся к идеальной обстановке и открытому пространству, а в реальных городских условиях практически невозможно проводить съем информации с расстояний, превышающих 10... 15 м на шумной улице, 15... 25 м — в остальных случаях. В загородных условиях — это 30...100 м. В принципе, необходимо запомнить простое правило: если оператор слышит речь своим ухом, но не может разобрать лишь отдельные слова, то с помощью хорошего направленного микрофона возможно осуществить перехват и звукозапись разговора; в противном случае никакой направленный микроф9н не поможет.

**В ПОМЕЩЕНИЯХ**

Отличительной особенностью применения направленных микрофонов в помещениях является более сложное звуковое поле полезного сигнала, которое представляет из себя суперпозицию составляющей «прямого» звука, созданной звуковыми волнами, не испытавшими ни одного отражения, и составляющих, созданных несколькими отраженными звуковыми волнами. Поле отраженных звуковых волн почти всегда близко к диффузному.

**Таблица 1.3.7. Уровни громкости различных источников шума**

| Источник шума и место его измерения | Уровень громкости, дБ |
|---|---|
| Громкий автомобильный гудок на расстоянии 8м | 95...100 |
| Электропоезд на эстакаде на расстоянии 6 м | 90 |
| Шум в поезде метро во время движения | 85...90 |
| Автобус (полный ход) на расстоянии 5 м | 85...88 |
| Трамвай на расстоянии 10-20 м | 80...85 |
| Троллейбус на расстоянии 5 м | 77 |
| Грузовой автомобиль на расстоянии 5-20 м | 60...75 |
| Легковой автомобиль на расстоянии 5-20 м | 50...65 |
| Шумная улица без трамвайного движения | 60...75 |

Обычный средний шум на улице /55...60
То же, в момент затишья днем /40
Тихая улица (без движения транспорта) /30...35
Тихий сад /20
Деревообрабатывающая фабрика /96...98
Зал при массовых сценах /75...95
Шумное собрание /65...70
Шепот на расстоянии 1 м /20
Разговор на расстоянии 1 м: громкий/обычный /65...70/55...60
Коридоры /35...40
Кафе /50...52

**Таблица 1.3.8. Предельные дальности акустической регистрации**

Вид деятельности / /Пределы слышимости, м
Шаги человека по грунту / /30...100
Громкий разговор / /200...300
Негромкий разговор / /100...200
Резкая команда голосом / /500...1000
Громкий крик / /1000...1500

Акустические шумы в помещениях так же, как и на открытой местности, существенно ограничивают динамический диапазон принимаемой информации, снижают разборчивость речи. Эти шумы создаются как людьми, так и вибрациями, проникающими в помещение извне (с улицы или из соседних помещений). Уровни шумов, создаваемые людьми, зависят от количества их в помещении, громкости разговоров и т. д. Уровни шумов (вибраций), проникающих снаружи, определяются звукоизоляцией помещения и уровнями внешних шумов.

В табл. 1.3.9 приведены санитарные нормы допустимых уровней акустических шумов, характерных для различных типов помещений. Приведенные цифры позволяют составить представления об условиях перехвата речевой информации с помощью направленных микрофонов. Здесь уместно еще раз напомнить, что уровень обычной речи на расстоянии 1 м составляет 65...75 дБ.

**Таблица 1.3.9. Уровни шумов, соответствующие санитарным нормам, для жилых и рабочих помещений**

Тип помещения /Норма, дБ
Для сна и отдыха /35
Для умственной работы без собственных источников шума (конструкторские бюро, комнаты программистов, лаборатории для теоретических работ и обработки экспериментальных данных) /45
Для конторского труда с источниками шума (принтеры), цеховой администрации, а также помещения, где источником шума являются люди (кассовые и справочные залы) /55
Производственные помещения, гаражи, механические мастерские /80

В общем случае лучшее качество перехвата информации в помещении обеспечивается при размещении направленного микрофона рабочей осью на источник сигнала (человека или группу людей), а тылом к источникам акустических помех. При этом оператор должен стремиться занять максимально тихое место (избегая углы, где особенно много переотраженных сигналов) в зоне действия прямого звука.

### 1.3.4. Диктофоны

Осуществление негласной (скрытой) звукозаписи является одним из наиболее распространенных приемов промышленного шпионажа. Полученные записи используют для получения односторонних преимуществ в коммерческих сделках, оказания давления на партнеров, шантажа и т. д.

Для того чтобы уберечь себя от подобных последствий, необходимо знать основные особенности скрытой звукозаписи, факторы, влияющие на качество фиксации информации, характерные приемы. Эти знания помогут обратить внимание на особенности поведения людей, пытающихся вас записать, правильно выбрать место конфиденциальной встречи, исключить нахождение «случайно забытых» вещей в вашем рабочем кабинете или офисе.

**Факторы, влияющие на качество звукозаписи**

При рассмотрении вопросов применения направленных микрофонов в реальных условиях

(п. 1.3.3) отмечалось, что работы на открытой местности и в замкнутом пространстве (помещении) различаются более сложными условиями для последнего случая. Рассмотрим его более подробно.

Звукозапись в помещении сопровождается большим количеством акустических помех, связанных, во-первых, с наличием переотраженных волн от внутренней обстановки помещения, а, во-вторых, с наличием шумов, создаваемых как людьми, так и шумами и вибрациями, проникающими в помещение извне (с улицы или из соседних помещений).

Акустическое поле в замкнутом объеме можно представить как сумму составляющих поля «прямого» звука, создаваемого звуковыми волнами, не испытавшими ни одного отражения, и составляющих поля, создаваемых отраженными звуковыми волнами. Поле отраженных звуковых волн почти всегда можно считать близким к диффузному, поэтому его часто называют диффузной составляющей.

Для оценки ее влияния на акустические свойства помещения, а следовательно и качество записи, вводят понятие акустического отношения для установившегося режима. Оно определяется как отношение суммарного уровня отраженных волн к уровню прямой волны.

В реальных условиях акустическое отношение для удаленных от источника звука точек помещения редко бывает меньше единицы, как правило, оно значительно больше, а иногда даже доходит до величины, равной 10...15. То есть уровень отраженных волн в помещении обычно выше уровня прямого звука. При акустическом отношении больше четырех отраженный звук создает недопустимые помехи для регистрации речевой информации.

Пороговое значение расстояния от источника звука, при котором акустическое отношение равно единице, называют радиусом гулкости, так как при большем расстоянии диффузная составляющая становится больше составляющей прямого звука, и в записанном сигнале появляется характерная гулкость.

Однако акустическое отношение полностью не характеризует качество восприятия звука в помещении, так как не все переотраженные сигналы вносят помехи, поэтому вводят еще одно понятие — четкость звучания. Под ним понимают отношение плотности энергии прямого звука (Епр), суммируемой с плотностью отраженных звуковых волн, приходящих в данную точку помещения в течение времени t = 60 мс после прихода прямого звука $E_{t=60\ мс}$ (и потому воспринимаемых с ним слитно), к общей плотности энергии Ет:

$$S_r = (E_{пр} + E_{t=60\ мс})/E_m.$$

То есть четкость звучания характеризует относительную величину всей полезной энергии Епол. В этом ее преимущество перед акустическим отношением. Чем больше четкость звучания, тем меньше влияние помех от запаздывающих лучей из-за явления реверберации. Однако на практике существуют большие трудности по измерению этой величины.

Как отмечалось выше, акустические шумы в помещениях существенно ограничивают динамический диапазон регистрируемой информации, снижают разборчивость речи. Степень их влияния зависит от количества людей в помещении, громкости разговоров, а также уровня шумов, проникающих извне.

В условиях тишины слышны писк комара, жужжание мухи, тиканье часов и другие звуки, а в условиях шума и помех можно не услышать даже громкий разговор. Другими словами, в условиях шума и помех порог слышимости для приема слабого звука возрастает. Это повышение порога слышимости называют акустической маскировкой. Величина маскировки определяется величиной повышения порога слышимости для принимаемого звукового сигнала.

К сожалению, внешние шумы не исчерпывают список помех, возникающих при негласной записи акустической информации. Дело в том, что закамуфлированный в одежде магнитофон записывает все окружающие его шумы, и в первую очередь создаваемые самим оператором, так как он, как правило, ближе всего расположен к микрофону. Так, например, люди дышат, а это значит, что одежда на них постоянно находится в движении — ремень поскрипывает от поднимающейся и опускающейся диафрагмы, пиджак трется о сорочку и т. д. Люди этого не слышат, однако, микрофон, спрятанный в одежде, улавливает все, и записанный разговор будет сопровождать невероятный фоновый шум.

Трудно представить себе, сколько различных звуков сопровождают нас, даже если

человек неподвижно застывает в кресле. Работа желудка и та создает помеху качественной записи, если «сосет под ложечкой». Конечно, может быть интересным сидеть и изучать изменения внутренних ритмов организма в зависимости от развития ситуации. Но кто сумеет распознать все прочее?

Самое большое неудобство для диктофонной записи — беседа на ходу. Здесь «фонит» все: рукава, трущиеся по мере размахивания руками, верхняя одежда, содержимое карманов (всякие ключики, мелочь, бумажки — все бряцает, шуршит и скрипит). Окружающие шумы также будут уловлены и записаны. И если в нормальной жизни мы их не слышим, используя данные природой фильтры, то при воспроизведении записи все будет воссоздано в самом неудобном виде.

Рассмотренные факторы являются принципиальными при проведении негласной звукозаписи, и они должны учитываться при выборе места для микрофона звукозаписывающего устройства.

**Выбор типа микрофона и места его установки**

Многие современные диктофоны позволяют выбирать между встроенным и выносным микрофонами в зависимости от условий ведения звукозаписи. Конечно, встроенный микрофон делает устройство более компактным и эргономичным. Однако его возможности по ведению скрытой фиксации аудиоинформации существенно ограничены, так как такие микрофоны обладают достаточно скромными характеристиками из-за предельно малых размеров, а их размещение полностью определяется размером и камуфляжем всего записывающего устройства.

Иначе обстоит дело с выносными акустическими приемниками. Они хорошо камуфлируются и поэтому могут быть установлены в зоне, обеспечивающей высокое качество записи. Выбору места возможного размещения и типа именно таких микрофонов следует уделить особое внимание.

При размещении выносных акустических приемников операторы, как правило, учитывают следующие нижеперечисленные три фактора.

КОЛИЧЕСТВО ЗАПИСЫВАЕМЫХ ИСТОЧНИКОВ РЕЧЕВЫХ СИГНАЛОВ

Для записи одного собеседника обычно применяют односторонне направленные микрофоны с расстояния 50—70 см. Реже используют и двусторонне направленные микрофоны (например, ленточные). Однако минимальная дальность до источника в этом случае возрастает до 80—100 см, так как на более близком расстоянии запись будет «бубнить».

Для фиксации диалога подходят как двусторонне, так и односторонне направленные микрофоны. В первом случае микрофон располагают между собеседниками, в последнем — его стараются установить так, чтобы оба объекта оказались симметрично расположенными относительно рабочей оси акустического приемника.

Для фиксации разговора нескольких собеседников чаще применяют односторонне направленные микрофоны с большим перепадом чувствительности по линии фронт—тыл. Их размещают таким образом, чтобы рабочая ось была направлена на собеседников, а тыл — в сторону источников акустических помех.

Для записи сцены «за круглым столом» чаще используют односторонне направленные микрофоны. В идеальном случае их размещают в центре в вертикальном положении с направлением нулевой чувствительности вниз.

ПРОСТРАНСТВЕННАЯ ОРИЕНТАЦИЯ МИКРОФОНА

Вообще пространственная ориентация определяется зависимостью чувствительности микрофона от угла между его рабочей осью и направлением на источник звука. Для большинства типов акустических приемников увеличение этого угла сопровождается падением как общей чувствительности, так и, в особенности, чувствительности на высоких частотах. Лишь у некоторых типов микрофонов, например, двусторонне направленных (восьмеричных) и в меньшей степени односторонне направленных, чувствительность на высоких частотах изменяется при повороте рабочей оси от направления так же, как и чувствительность на низких частотах. Поэтому микрофоны направляются своей рабочей осью не на источник только в тех случаях, когда надо сделать запись этого звука менее громкой на фоне других или же придать звучанию большую мягкость и меньшую четкость.

ДАЛЬНОСТЬ ДО ИСТОЧНИКА АКУСТИЧЕСКОГО СИГНАЛА

Величина расстояния до источника определяется, исходя из свойств помещения, в котором осуществляется аудиозапись, и свойств микрофона и источника.

Акустические процессы в каждой точке помещения довольно хорошо, как отмечалось выше, определяются величиной акустического отношения. Восприятие же источника в нем зависит от того, в каком соотношении находятся расстояние от источника до микрофона и радиус гулкости помещения.

Если расстояние от источника до микрофона меньше радиуса гулкости, то при воспроизведении кажущиеся размеры источника звука больше фактических, а размеры окружающего пространства меньше фактических. При этом создается общее впечатление близости и интимности звучания. При расстоянии микрофона от источника больше радиуса гулкости, наоборот, размеры источника кажутся меньше фактических, а окружающего пространства — больше. Общее впечатление от звучания — объемность, «воздушность», мощность. При расположении микрофона от источника звука на расстоянии, равном радиусу гулкости, качество звучания при воспроизведении является промежуточным по сравнению с описанным выше.

**Средства обеспечения скрытности оперативной звукозаписи**

Выше отмечалось, что в зависимости от используемой модели диктофон может иметь встроенный или выносной микрофон.

Первый существенно уступает последнему по техническим характеристикам, а кроме того имеет меньшие возможности по скрытому применению. Поэтому на практике чаще используют выносные акустические приемники.

Выносной микрофон может быть закамуфлирован под любой элемент личных вещей. Часто он изготавливается в виде пуговицы и вставляется в петлицу на одежде. А так как пуговицы взаимозаменяемые, то достаточно просто провести общую маскировку из предлагаемого ассортимента. Например, стандартный вариант — белая пуговица на светлой рубашке.

Широко применяются и выносные микрофоны в виде колпачка от авторучки, заколки для галстука и других предметов (как правило, они не вызывают никаких подозрений).

Более простые устройства не имеют штатного камуфляжа, а благодаря своим небольшим размерам прячутся под одежду или в различных предметах (книге, папке, портфеле). В зависимости от типа используемого диктофона и расстояния от источника звука микрофоны могут оборудоваться дополнительным усилителем. Как правило, это делается в том случае, если микрофон устанавливается на значительном расстоянии от диктофона.

Необходимо упомянуть о миниатюрных диктофонах, которые используются для скрытной записи. Так, если ранее (в 30—50-е годы) наименьший размер магнитофона позволял разместить его в портфеле или папке, то в настоящее время не составляет труда приобрести в обычном магазине диктофон, который свободно помещается в пачке сигарет. Наиболее часто в интересах промышленного шпионажа применяются диктофоны типа **SONY-909M**, **SONY-950**, **NATIONAL-RNZ-36**, **OLYMPUS-L400**. К сожалению, часть устройств не снабжена внутренним динамиком, поэтому прослушивание записи в них приходится осуществлять через внешний акустический блок или наушники.

Микрокассета МС-90 позволяет обеспечивать до б часов непрерывной записи. Некоторые диктофоны снабжены беззвучным автостопом, большинство — системой VOX (автоматического включения записи при появлении источника акустического сигнала — акустомат), выносным микрофоном и системой дистанционного включения/выключения. Стоимость подобных изделий составляет от 200 до 500 $.

Иногда для несанкционированной записи используются и такие простые изделия, как **OLIMPUS-S928** или **SONY-359**, цена которых составляет от 35 до 100 $. Правда, и качество записи у этих моделей похуже, к тому же изделия такого класса часто не имеют гнезда для подключения выносного микрофона.

В ряде случаев используют и магнитофоны, имеющие увеличенные по сравнению с описанными выше диктофонами габариты. Они, как правило, соответствующим образом маскируются или используются для дистанционной записи, а фиксация информации в них осуществляется на стандартную кассету, как, например, в диктофонах РК660 и РК670. Некоторые устройства имеют автореверс и пониженную скорость протяжки, что позволяет обеспечивать длительное время записи, особенно на кассеты типа С-120 (естественно, за счет ухудшения качества записи). Основное достоинство в использовании стандартных кассет — это возможность прослушивания на обычной бытовой аппаратуре. Стандартным вариантом камуфляжа для РК660 и РК670 является книга со специальным вырезом для акустического сигнала.

Все основные типы портативных диктофонов, используемых в интересах промышленного шпионажа, отвечают, как правило, следующим требованиям к техническим характеристикам: диапазон частот — от 200...300 Гц до 3...5 кГц, коэффициент детонации (коэффициент колебания скорости ленты) — до 4 %, остаточный уровень шумов — 30 дБ, коэффициент гармоник — до 10%, разборчивость слогов — 60...80% при доверительной вероятности не хуже 0,9.
Некоторые марки современных диктофонов и их технические возможности приведены в табл. 1.3.10, а внешний вид — на рис. 1.3.36.


**Рис. 1.3.36. Современные малогабаритные диктофоны, применяемые в интересах промышленного шпионажа:**
а — OLIMPUS- L250; 6 — OL1MPUS-S950; в — OLIMPUS-L400; г — цифровой диктофон VR-5000
Однако закамуфлированное размещение выносного микрофона и самого диктофона не исчерпывает **проблем скрытой звукозаписи**, поэтому важно знать, с какими проблемами сталкиваются ваши недобросовестные конкуренты и как они их могут решить:
>- некоторые диктофоны имеют неприятные особенности управления - выключаться с характерным щелчком выстреливаемых кнопок или после окончания кассеты включать обратную перемотку, что также может вылиться в нежелательные последствия. Бывают экземпляры с программируемым управлением и таймером, автоматически включающиеся на воспроизведение в самый неподходящий момент (поэтому если во время разговора у вашего собеседника в кармане что-то щелкнуло, то будьте готовы к тому, что вся предыдущая беседа уже на пленке);
>- другой важной проблемой является емкость записи. Поэтому человек, осуществляющий скрытую аудиозапись, вынужден постоянно следить за временем беседы для того, чтобы не выйти за кассетное время. Это иногда весьма неудобно. Для увеличения времени записи в некоторых диктофонах, как отмечалось выше, используется пониженная скорость лентопротяжного механизма (меньше 1,2 см/с), но качество записи при этом, как уже отмечалось, существенно ухудшается и иногда даже становится проблематично идентифицировать разговор;
>- низкое качество звукозаписи в силу различных ранее упомянутых причин (акустические помехи и т. п.).
**К основным путям решения указанных проблем** относятся следующие. Для того чтобы избежать неприятностей с обнаружением факта негласной звукозаписи из-за щелчков и переключений в диктофоне, в первую очередь идут по пути использования

профессиональных средств, специально предназначенных для скрытой аудиозаписи. К ним относятся, например, диктофоны типа **UHER CR-1600, UHER CR-1601, MARANTZ PMD-201, MARANTZ PMD-221.** Их основные характеристики приведены в табл. 1.3.11. Главный недостаток — очень высокая цена, которая может достигать нескольких тысяч долларов. Другой путь — использование магнитофонов с электронной записью звука. Например, диктофон **Edic** способен непрерывно вести фиксацию акустических сигналов в течение 1...2 суток, сохраняя последние 20—40 мин записи. Диктофон незаменим для звуковой регистрации неожиданных ситуаций, так как нет необходимости нажимать кнопку пуска при внезапном интересе к какой-либо информации, она автоматически запишется и будет храниться до 40 мин, пока не «затрется» новой записью. Единственное неудобство для оператора — надо не забыть нажать на «стоп» после окончания интересующего разговора. Небольшие габаритные размеры (105x55x14 мм) позволя

**Таблица 1.3.10. Технические характеристики некоторых современных диктофонов**

Характеристика /UHER-MC 8SL /DICTAPHONE-1254 /SONY M-950 /VOICE-IT VR-5000 (цифровой) /OLIMPUS S926 /
Акустомат /+ /+ /+ /+ /+ /
Изменение чувствительности микрофона / /+ /+ / /+ /
Кнопка паузы /- /+ /+ /+ /+ /
Автореверс /- /- /+ /- /- /
Разъем микрофона /+ /+ /+ /+ /- /
Разъем наушника /- /+ /+ /+ /+ /
Разъем ДУ /- /- /+ /- /- /
Индикатор работы/жидкокристаллический дисплей (ЖКД) /+/- /+/+ /+ /-/+ /+/- /
Счетчик ленты /- /+ /+ /+ /- /
Быстрое стирание /мини /МИНИ /микро /Встроенная память + чип /- /
Запись времени /+ /- /- /+ /- /
Ускоренное воспроизведение /+ /+ /+ /+ /+ /
Быстрая перемотка /1 /1 /2 /2 /+ /
Автостоп /+ /+ /+ /+ / /
Полный автостоп /металл /металл /металл /пластмасса /+ /
Источник питания /1x9В /2ААА /1ААА /2ААА /2x1,5 ВАА батарея /
Габариты, мм /20x54x129 /18x54x128 /67,6x64.6x18.5 /120x55x24 /122x57x24 /
Вес (вес с батарейками), г/200/190/100//160/

/OLIMPUS S928 /OLIMPUS S950 /OLIMPUS S830 /OLIMPUS L200 /OLIMPUS L400 /DT1000 (цифровой)
/+ /+ /- /+ /+ /
/+ /+ / / /+ /При использовании ДУМК9
/+ /+ /- /+ /- /-
/- /- /- /- /+ /-
/+ /+ /+ /+ /+ /+
/+ /+ /+ /+ /+ /+
/+ /- /- /- /+ /+
/+/- /+/+ /+/- /+/- /-/+ /На ДУ MR9
/+ /+Р(ЖКД) /+/+ /+(ЖКД) /+
/- /- /- /- /- /+
/- /+ /- /- /- /-
/+ /+ /- /+ /- /+
/+ /+ /+ /- /- /+
/ / / /+ / /Сигнализация об окончании работы
/+ /+ /+ / /+ /Сигнализация об окончании кассеты
/2x1,5 ВАА батарея /2Х1.5ВАА батарея /2x1,5ВАААА батарея /2x1,5 В ААА батарея /1x1,5 В ААА батарея /Адаптер 9В/800 мА
/122x57x24 /120x58x24 /110x56x18 /107x51x15 /73x52x20 /240x78x170
/160 /173 /140 /125 /90 /800

**Таблица 1.3.11. Технические характеристики профессиональных кассетных магнитофонов**

Технические характеристики /UHER CR-1600 /UHER CR-1601 /MARANTZ PMD-201 /MARANTZ PMD-221

Скорость движения ленты, см/с /4,7; 1,2 /4,7; 2,4; 1,2 /4,7; 2,4 /4,7; 2,4

Диапазон рабочих частот, Гц / / / /

для скорости 4,7 см/с /300... 16000 /300... 16000 /40...14000 /40... 15000

для скорости 2,4 см/с /— / /40... 8000 /40...8500

для скорости 1,2 см/с /600...3400 /600...3400 /— /—

Отношение сигнал/шум /70 /70 /57 /57

Длительность перемотки, с /90 /90 / /

Количество головок, шт /2 /3 (сквозной канал) /2 /3 (сквозной канал)

Режим работы /стерео /моно / /

Размеры, мм / / /228x51x165 /228x51x165

Масса, кг / / /1,3 /1,3

ют легко камуфлировать диктофон. В нем нет движущихся частей, поэтому его применение сложно обнаружить. Комплектуется выносным микрофоном и зарядным устройством для встроенных аккумуляторов.

Более современными вариантами являются малогабаритные цифровые стереофонические диктофоны **NT-1** и **NT-2** фирмы SONY. Главное достоинство данных устройств — наличие специальных бесшумных кнопок и высокое качество записи. Дополнительные возможности создает встроенный календарь и часы, автоматически регистрирующие и сохраняющие время начала и конца записи.

Для увеличения времени непрерывной записи используют реверсивные системы. Однако и здесь не каждая модель может быть использована, так как при переключении записи на реверс некоторые диктофоны (а их, к сожалению, большинство) издают довольно громкий щелчок, о чем говорилось выше.

Иногда для экономии ресурсов используют функцию включения по голосу — акустомат (см. п. 1.3.1). Но здесь, как и у закладного устройства, «съедается» начало первой фразы. Если порог срабатывания выставлен некорректно, то возможен пропуск целых предложений.

Для экономии рабочего тела (пленки) в ряде случаев используется система дистанционного включения. В простейшем случае она представляет собой переключатель, соединенный проводом с соответствующим разъемом на диктофоне, а при отсутствии специального разъема используется доработанный вход по питанию. Система внешнего включения должна содержать переключатель с четкой фиксацией положения, чтобы в стрессовых ситуациях оператор был уверен, что его диктофон действительно работает. Иногда используют специальные системы включения, например, в виде зажима для авторучки. В случае, когда авторучка находится в зажиме, расположенном во внутреннем кармане, диктофон выключен, а когда она извлечена — производится запись.

Некоторого преимущества при использовании диктофонов позволяет достичь применение дистанционного включения по радиоканалу. Данная техника предназначена для применения устройств аудиозаписи в качестве закладки (п. 1.3.1). Запуск диктофона производится специальной командой, передаваемой радиопередатчиком. Например, устройство дистанционного управления **РК1670** имеет передатчик мощностью 1 Вт и дальность действия 500 м. Габариты приемника команд — 25x58x18 мм, вес — всего 55 г. Подключается приемник к соответствующему разъему магнитофона.

Существенно увеличить время непрерывной звукозаписи позволяет использование диктофонов с записью на жесткий проволочный носитель, изготовленный из специальных сплавов. Их память может простираться на сутки и более. Однако в будущем они, видимо, не найдут широкого применения для вышеуказанных целей. Это связано в первую очередь с такими недостатками, как трудность соединения проволоки при монтаже и обрывах, появление паразитной амплитудной модуляции сигнала из-за скручивания носителя, неудовлетворительная передача верхних частот, довольно высокая стоимость, сильный износ головок.

Перспективным по-прежнему остается применение цифровых диктофонов. Тем более, в последнее время появились диктофоны нового типа — с записью в память персональной ЭВМ.

Например, цифровая система регистрации переговоров **«Аудиокод»**. Данная система

предназначена для записи информации, ее сжатия (компрессии), хранения с автоматическим удалением устаревших материалов и прослушивания информации. Область фиксируемых звуковых частот канала «запись—воспроизведение» лежит в диапазоне 300...3000 Гц. Система защищена от несанкционированного доступа. Обеспечивается одновременная регистрация переговоров по 4 каналам с автоматической или ручной регулировкой уровня записи в каждом канале, реализована функция «эхо» (прослушивание записываемых каналов). Включение записи осуществляется по уровню входного сигнала или после нажатия клавиши. Кроме того, в диктофоне предусмотрен мгновенный доступ к любой записи базы данных, быстрый поиск по номеру канала и времени регистрации, прослушивание любой записи без прерывания процесса регистрации, воспроизведение с любого места, **быстрый** переход к **любому** участку фонограммы.

Для обеспечения цифровой записи в различных марках диктофонов используются различные форматы записи. К наиболее известным относятся следующие.

**DAT** (Digital Audio Tape) — формат цифровой магнитной записи звука на специальную DAT-кассету, время непрерывной работы которой достигает двух часов, а в режиме Long Play (LP) — четырех часов. Запись ведется вращающимися головками, как в видеомагнитофонах, а магнитная лента движется со скоростью всего 8,15 мм/с.

Исходный аналоговый сигнал преобразуется в цифровую форму и **без** сжатия записывается на ленту. Запись, сделанная на DAT-магнитофоне, отличается малым уровнем шумов, большим частотным и динамическим диапазоном, что обеспечивает высокое качество звука, зачастую превосходящее качество компакт-диска. Однако широкому распространению этих аппаратов помешала их высокая цена. Поэтому DAT-магнитофоны нашли применение только в профессиональной звукозаписи: на них, например, записывают мастер-ленты для изготовления компакт-дисков. Некоторые фирмы сейчас выпускают портативные DAT-магнитофоны, которые можно использовать в качестве диктофонов для получения высококачественной записи речи. Причем полоса записываемых частот настолько широка, что позволяет делать записи в режиме LP без заметного снижения качества звучания, а продолжительность записи при этом увеличивается вдвое. Кроме высокой стоимости самого аппарата и DAT-кассет, к недостаткам DAT-магнитофонов относится сравнительно быстрый износ механизма протяжки из-за высоких требований к нему по скорости перемотки и поиску интересующих фрагментов. Цена бытовых аппаратов —700 $ и выше. Основные производители DAT-магнитофонов — Pioneer, Sony, Tascam.

**DCC** (Digital Compact Cassete) — цифровая компакт-кассета (изобретение фирмы Philips), выпущенная на рынок в 1992 году. Основным достоинством DCC-системы является полная совместимость с обычными компакт-кассетами. Цифровая звукозапись ведется с помощью стационарной многодорожечной головки при стандартной скорости протяжки ленты, при этом исходный звуковой сигнал подвергается многократному сжатию с помощью адаптивного алгоритма, учитывающего психологические особенности восприятия звука человеком. Стоимость первых образцов DCC-магнитофонов также оказалась высокой, а качество звука довольно низким, и это решило их судьбу — они не нашли широкого применения. Качество звучания впоследствии удалось существенно улучшить, однако доверие к новой системе было подорвано. Сейчас фирма Philips производит DCC-магнитофо-ны, в том числе и портативные, которые можно приобрести в магазинах по цене от 700 $. Несомненный интерес представляет возможность воспроизводить на этих аппаратах записи, сделанные на компакт-кассетах обычным способом. Однако ограниченное распространение этого формата затрудняет его внедрение в практику.

**MD (Mini Disc)** -— мини-диск — разработан фирмой Sony. Конструктивно он напоминает 3,5-дюймовую компьютерную дискету диаметром 64 мм. Материал, из которого изготовлен диск, меняет свои оптические свойства под воздействием магнитного поля. Запись на мини-диск осуществляется магнитной головкой, при этом поверхность диска в зоне действия магнитного поля разогревается лучом лазера. Считывание информации происходит также с помощью лазера, но меньшей мощности. Таким образом, информация сохраняется на диске даже в случае воздействия сильных магнитных полей и появляется возможность многократной (до 1 млн раз) перезаписи. На мини-диск можно записать стереозвук продолжительностью до 74 мин, а некоторые модели мини-дисковых аппаратов позволяют вести монофоническую запись в течение 148 мин.

Разработчиками формата применен адаптивный алгоритм сжатия и кодирования информации — ATRAC (подобный используемому в DCC-маг-нитофонах). Благодаря его постоянному совершенствованию качество звука приближается к уровню качества записи на компакт-диске. Минидисковая аппаратура успешно применяется в студиях звукозаписи, на радио, в любительской звукозаписи. Некоторые фирмы выпускают малогабаритные мини-дисковые плееры с возможностью записи. Их стоимость находится в пределах 350—450 $. Производители — Sony, Pioneer, Kenwood, Denon, Aiwa.

**CD-R, CD-RW** — записываемый компакт-диск. Первый CD-рекодер был разработан фирмой Pioneer в 1996 году. В нем был применен записываемый компакт-диск с возможностью однократной записи (CD-R). Существует несколько технологий однократной записи цифровых данных на компакт-диск. Одна из них использует эффект химических превращений в органическом красителе под действием лазерного луча. По другой технологии луч сравнительно мощного лазера просто прожигает отверстия в тончайшем слое металла. Совсем недавно фирмой Philips и некоторыми другими были разработаны и выпущены в продажу CD-рекодеры с возможностью многократной перезаписи на компакт-диск (CD-RW). Продолжительность записи на эти диски обычно не превышает 74 мин. В продаже представлены CD-R и CD-RW рекодеры в стационарном исполнении, так как они в основном предназначены для копирования компакт-дисков, и записывающие CD-ROM для компьютеров. Поэтому этот формат представляет интерес в тех случаях, когда уже имеется соответствующее оборудование для воспроизведения компакт-дисков или CD-ROM.

**NT (Non Tracking)** — бездорожечный принцип записи на специальную микрокассету — разработан и реализован фирмой Sony в диктофонах NT-1 и NT-2 (рис. 1.3.37). В них запись производится вращающимися со скоростью 3000 об/мин головками на ленту шириной 2,5 мм, которая движется со скоростью 6,35 мм/с. Это обеспечивает запись стереозвука в диапазоне 10... 14 000 Гц при соотношении сигнал/шум 80 дБ. Цифровой звуковой сигнал записывается без сжатия. Продолжительность записи составляет 60, 90 и 120 минут в зависимости от типа микрокассеты. Диктофон весит 147 г, имеет габариты 113x23x55 мм. К недостаткам диктофонов следует отнести их высокую стоимость.

**Незаметный прибор звукозаписи STG 1105 —** миниатюрный прибор скрытой звукозаписи с размерами кредитной карточки, рассчитан на непрерывную звукозапись с двумя скоростями в течение 4 ч и может воспринимать слабые аудиосигналы. Последние управляют автоматическим включением и выключением внешнего усилителя/громкоговорителя. Прибор имеет регулятор тона и индикатор напряжения батареи электропитания. С прибором используются высоконаправленный микрофон Mini-Shotung STG 1411 и микрофон STG 1413, закрепляемый на лацкане пиджака или куртки. При использовании любого из этих микрофонов обеспечивается запись высокого качества. В комплект принадлежностей прибора входит соединительный шнур для его подключения к радиоприемнику STG 4401 PXP2-U.

**Технические характеристики**

Размеры,мм..... 85x50x12
Масса, г ..... 110 с батареей
Электропитание прибора..... один элемент типа ААА, 1,5 В,
блок электропитания от сети переменного тока напряжением 110/220 В;
Электропитание громкоговорителя .... два элемента типа АА, 3 В

Для улучшения разборчивости речи, полученной в результате скрытой звукозаписи, используют различные очищающие фильтры. Они особенно эффективны, если фиксация информации осуществлялась на фоне мощных, но сосредоточенных по спектру помех или специфически окрашенных шумов.

**Рис. 1.3.37. Цифровой диктофон NT-2 фирмы Sony**

В простейшем случае можно использовать широко известные эквалайзеры. Однако часто этот прием не помогает, поэтому применяют специально разработанные устройства.
Например, цифровой нелинейный адаптивный фильтр **АФ-512** специально предназначен для обработки зашумленных речевых сигналов в реальном масштабе времени. Его рабочая полоса лежит в пределах от 200 до 5000 Гц, а коэффициент нелинейных искажений не превышает 0,5 %, габариты — 300х200х80 мм. При обработке записей на фоне сосредоточенных помех фильтр позволяет увеличить разборчивость речи в 1,5... 5 раз. Правда, фильтр недостаточно эффективен, если помехой будут быстрая музыка, шум, речь.
Более совершенными являются специальные программно-аппаратные комплексы очистки речи; например «Золушка-97». Это двухканальное цифровое устройство шумоочистки речевых сигналов. Оно предназначено:
>- для очистки «живого» звука и звукозаписей;
>- для повышения разборчивости и качества речи в условиях низкого качества каналов связи;
>- для выделения источника звука в условиях «шумного» производства.
При его применении обеспечивается обработка сигналов с изменяющимися во времени характеристиками шумов, одновременное устранение нескольких типов помех, использование свойств восприятия (психоакустики) при расшифровке текста и некоторые другие возможности.

### 1.3.5. Устройства, реализующие методы высокочастотного навязывания

#### Общая характеристика высокочастотного навязывания

Под высокочастотным навязыванием (ВЧ-навязыванием) понимают способ несанкционированного получения речевой информации, основанный на зондировании мощным ВЧ-сигналом заданной области пространства.
Он заключается в модуляции электромагнитного зондирующего сигнала речевым в результате их одновременного воздействия на элементы обстановки или специально внедренные устройства.
Качество перехвата аудиоинформации с помощью ВЧ-навязывания зависит от ряда факторов:
>- характеристик и пространственного положения источника акустического сигнала;
>- наличия в контролируемом помещении нелинейного элемента (устройства), параметры которого (геометрические размеры, положение в пространстве, индуктивность, емкость, сопротивление и т. д.) изменяются по закону акустического сигнала;
>- характеристик внешнего источника, облучающего данный элемент (устройство);
>- типа приемника отраженного сигнала.
Принцип организации съема информации, основанный на зондировании, показан на рис. 1.3.38. Однако в некоторых случаях применяются и более сложные схемы.
Основные достоинства данного способа заключаются в активации модуляторов ВЧ-сигнала (нелинейных элементов) только на момент съема информации, а также в возможности (в ряде случаев) вести акустический контроль помещений без непосредственного проникновения для установки закладных устройств.
Недостатки: как правило, малая дальность действия и высокие уровни облучающих сигналов, наносящие вред здоровью людей. Данные обстоятельства существенно снижают ценность ВЧ-зондирования. Однако определенные методы, о которых будет рассказано в дальнейшем, получили достаточно широкое распространение.


**Рис.1.3.38. Организация перехвата акустической информации с использованием ВЧ-навязывания**

Общее представление о многообразии методов такого перехвата дает рис. 1.3.39, отражающий следующую их классификацию.
>- по диапазону частот:
радио;
оптические;
>- по среде распространения:
по токопроводящей среде;
через диэлектрик (воздух);
>- по использованию специально внедренных на объект устройств:
с внедрением;
дистанционные;
>- по оперативности получения результатов;
в реальном масштабе времени;
с временной задержкой.
Рассмотрим некоторые из принципов ВЧ-навязывания, описанных в доступной литературе.


**Рис. 1.3.39. Виды методов перехвата аудиоинформации с использованием ВЧ-навязывания**

**Устройства для перехвата речевой информации в проводных каналах**

В настоящее время ВЧ-навязывание нашло широкое применение в телефонных линиях для акустического контроля помещений через микрофон телефонной трубки, лежащей на аппарате.

Принцип реализации метода заключается в том, что в телефонную линию относительно общего корпуса (в качестве которого, например, используют контур заземления или трубы парового отопления) на один из проводов подают ВЧ-колебания от специального генератора-передатчика (ПРД). Через элементы схемы телефонного аппарата (ТА), даже если трубка не снята, они поступают на микрофон и модулируются речью ничего не подозревающих собеседников (рис. 1.3.40).

Прием информации производится также относительно общего корпуса, но уже через второй провод линии. Амплитудный детектор приемника (ПРМ) позволяет выделить низкочастотную огибающую для дальнейшего усиления и записи. Очевидно, что качество перехватываемой информации тем выше, чем ближе осуществлено подключение к телефонному аппарату (оконечному устройству). Это обстоятельство вносит определенные неудобства в использование данного метода. Фильтр нижних частот (ФНЧ) в линии необходим для одностороннего распространения высокочастотных зондирующих колебаний.

Принципиально ВЧ-сигнал в данном случае используется для преодоления разомкнутых

контактов микрофонной цепи аппарата при положенной телефонной трубке. Дело в том, что для зондирующего сигнала механически разомкнутый контакт является своего рода воздушным конден-

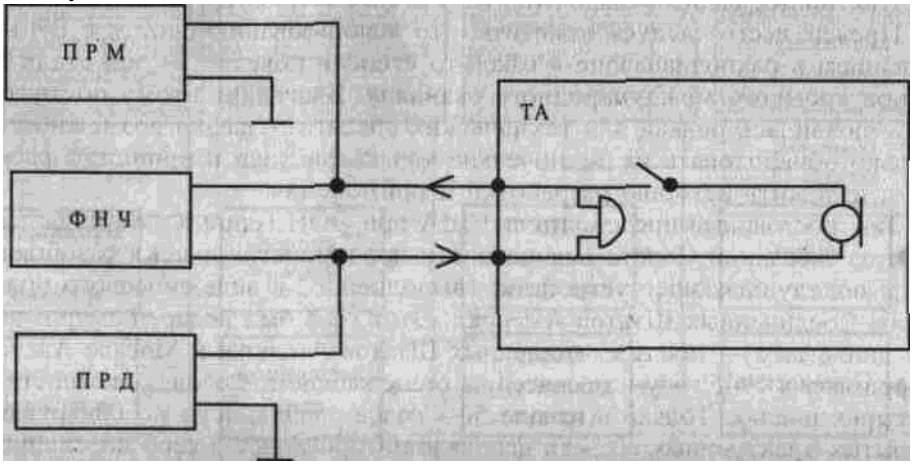



**Рис. 1.3.40. Принцип реализации ВЧ-навязывания на телефонный аппарат**

сатором, сопротивление которого будет тем меньше, чем выше частота сигнала от генератора.

При воздействии ВЧ-излучения на телефонный аппарат нелинейные процессы происходят в целом ряде элементов его электрической схемы. Однако наиболее сильно они проявляются именно в микрофоне, сопротивление которого изменяется по закону случайно воздействующего акустического сигнала, что и приводит к амплитудной модуляции несущей. Для гарантированного возникновения указанного эффекта уровень зондирующего сигнала в микрофонной цепи должен быть не меньше 150 мВ, а выходное сопротивление генератора должно быть выше, чем у микрофона, в 5—10 раз. Частота зондирующего сигнала должна лежать в диапазоне 30 кГц... 20 МГц. Чаще ее выбирают примерно равной 1 МГц, так как при этом обеспечиваются наилучшие условия распространения.

Схема устройства, реализующего вышеописанный метод, приведена на рис. 1.3.41. В ней умышленно отсутствуют номиналы элементов, что не позволяет реализовать ее на практике.

Дальность действия подобных устройств в реальных условиях не превышает нескольких десятков метров.

В перспективе в области использования проводных каналов, вероятно, будут осваиваться способы зондирования не только телефонных аппаратов, но и других устройств, в том числе по цепям питания, заземления и т. д.

**Перехват речевой информации с использованием радиоканала**

О работе устройств, использующих принцип ВЧ-навязывания через электромагнитное поле частично уже упоминалось при описании пассивных и полуактивных радиозакладок (п. 1.3.1). Рассмотрим их более подробно.

Прежде всего следует отметить, что использованию систем с ВЧ-навязыванием в радиодиапазоне в какой-то степени повезло — они стали причиной громкого международного скандала. Благодаря этому обстоятельству появилась редкая для технических средств разведки возможность не только обнародовать их технические характеристики и принципы работы, но и изложить историю разработки и применения.

Так, постоянный представитель США при ООН Генри Кэбот Лодж на одном из заседаний Совета Безопасности продемонстрировал в разобранном виде подслушивающее устройство, выполненное в виде гипсового орла — герба Соединенных Штатов Америки. Этот герб был подарен американскому дипломату — послу Соединенных Штатов Америки в Москве Авереллу Гарриману в 1945 году и провисел на стене кабинета в общей сложности при четырех послах. Только в начале 50-х годов специалисты по обнаружению скрытых электронных средств нашли вмонтированное в герб подслушивающее устройство. Инициатор создания программы ЦРУ по разработке миниатюрных средств оперативной техники Питер Карлоу вспоминает, что «мы

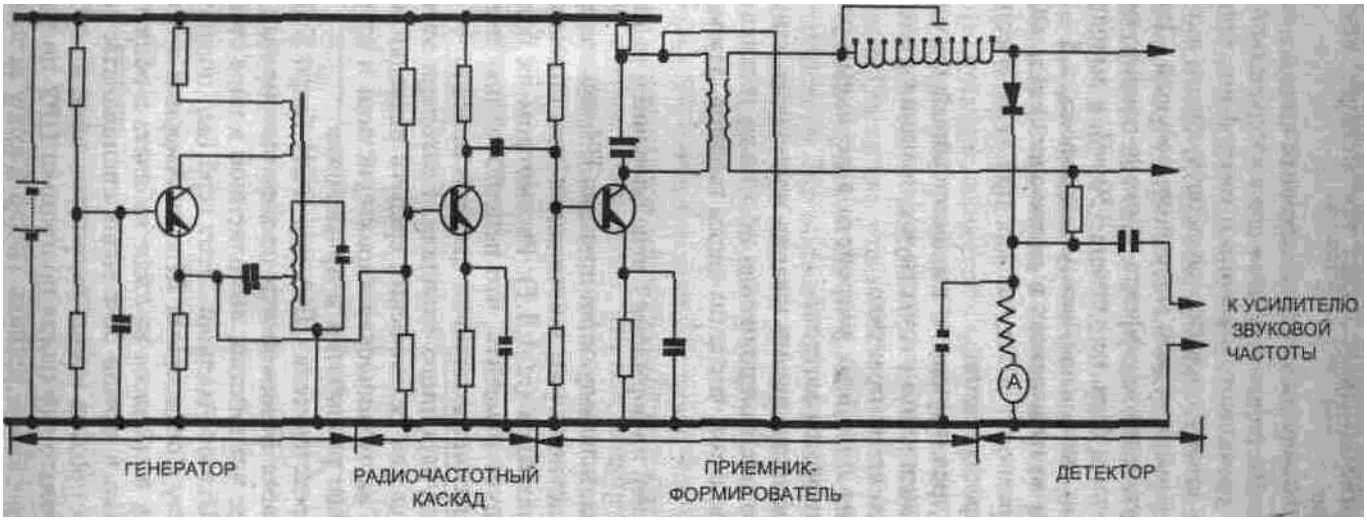


Рис. 1.3.41. Схема высокочастотного устройства перехвата речевой информации через телефонный аппарат

нашли его, но долго не знали принцип действия. В гербе находилось пассивное устройство, похожее на головастика с маленьким хвостом».

Таким образом, долгое время советское руководство имело возможность получать актуальную, очень важную оперативную информацию, что давало нам определенные преимущества в прогнозировании и осуществлении мировой политики в сложный период «холодной войны».

Имеются данные о том, что, даже зная, что в кабинете посла находится подслушивающее устройство, специалисты обнаружили его только тогда, когда вынесли из кабинета практически всю мебель. В наших разведывательных кругах ходили тогда слухи, что первые подозрения появились у американцев после одной из речей Н. С.. Хрущева, когда в результате анализа сведений, высказанных им, специалисты пришли к выводу, что источник утечки информации находится в посольстве США в Москве.

Опубликование информации о необычном закладном устройстве явилось сенсационным еще и потому, что США было заявлено об отсутствии у них аналогичной спецтехники. Она явилась для них полной неожиданностью. Также сообщалось, что Соединенные Штаты приступили к разработке подобных систем съема информации. И действительно через много лет американцы создали у себя аналогичный вид техники съема информации, который и внедрили в советское посольство за рубежом.

Автором и ведущим руководителем проекта первого пассивного закладного устройства был выдающийся изобретатель Лев Сергеевич Термен. Большой Энциклопедический Словарь уделил ему несколько строк. Родился в 1896 году. Советский физик. Музыкант. В 1920 году изобрел электромузыкальный инструмент «Терменвокс». В 1931—1938 годах — директор акционерного общества по производству электромузыкальных инструментов в США. С 1966 года — научный сотрудник кафедры МГУ. Известно, что Л. С. Термен лично демонстрировал В. И. Ленину свой инструмент, основанный на изменении тона звука генератора при поднесении рук к двум антеннам. В начале 30-х годов Термен после поездки остался в Америке, где основал акционерное общество. Помимо изготовления музыкальных инструментов он участвовал в оборудовании границы между США и Мексикой системой охранной сигнализации для регистрации незаконного пересечения границы нелегалами-мексиканцами. Принцип действия сигнализации такой же, как и аппарата «Терменвокс», емкостной, то есть основывался на регистрации изменений электрической емкости провода, натянутого вдоль границы, при приближении к нему человека.

Когда Термен перед войной приехал туристом в СССР, он, по приказу Берии, был арестован и отправлен в организацию, подобную той, которая была описана А. И. Солженицыным в романе «В круге первом» под названием «шарашка». В эти годы (в середине 40-х) Л. С. Термен и создал свой шедевр, которым до сих пор не устают восхищаться специалисты (рис. 1.3.42).

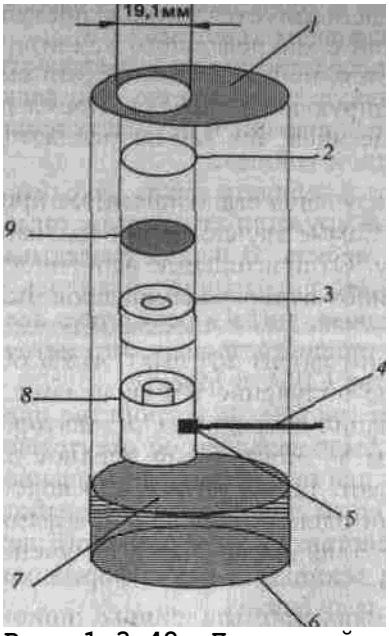



**Рис. 1.3.42. Пассивный радиомикрофон:**

1 — верхняя пластмассовая крышка; 2 — ферритовое кольцо; 3 — изолятор; 4 — антенна (четвертьволновой вибратор); 5 — согласующий конденсатор; 6 — корпус; 7 — жидкость; 8 — медный цилиндр (индуктивность); 9 — металлическая диафрагма

Основой устройства является цилиндрический объемный резонатор, на дне которого налит небольшой слой масла. Верхняя часть закрыта крышкой из пластмассы, являющейся прозрачной для радиоволн, но препятствующей проникновению акустических колебаний. В крышке имеется отверстие, через него внутренний объем резонатора сообщается с воздухом помещения, в котором ведутся переговоры. В указанное отверстие вставлена металлическая втулка, снабженная четвертьволновым вибратором, настроенным на частоту 330 МГц. Размеры резонатора и уровень жидкости подобраны таким образом, чтобы вся система резонировала на внешнее излучение с частотой 330 МГц. При этом собственный четвертьволновый вибратор внутри резонатора создает внешнее поле переизлучения. При ведении разговоров вблизи резонатора на поверхности масла появляются микроколебания, вызывающие изменение добротности и резонансной частоты резонатора. Этих изменений достаточно, чтобы влиять на характеристики переизлученного поля, создаваемого внутренним вибратором. Сигнал становится модулированным по амплитуде и фазе акустическими колебаниями. Работать такой радиомикрофон может только тогда, когда он облучается мощным источником на частоте резонатора, то есть 330 МГц.

Главным достоинством такого радиомикрофона является невозможность его обнаружения известными средствами поиска радиозакладок при отсутствии внешнего облучения.

Наряду с пассивными закладками, аналогичными выше описанной, для съема информации используются и полуактивные закладки, называемые аудиотранспондерами; (ответчиками; Audiotransponder). К таким закладкам относятся, например, SIM-ATP-16, SIM-ATP-40 (Hildenbrand-Elektronik), PK.500 (PK-Elektronik) и некоторые другие.

Транспондеры начинают работать только при облучении их мощным узкополосным высокочастотным зондирующим (опорным) сигналом. Приемники транспондеров выделяют зондирующий сигнал и подают его на модулятор, где, как правило, осуществляется узкополосная частотная модуляция сигнала. В качестве модулирующего используется сигнал, поступающий или непосредственно с микрофона, или с микрофонного усилителя. Промодулированный ВЧ-сигнал переизлучается, при этом его частота смещается относительно несущей частоты зондирующего сигнала. Время работы транспондеров составляет несколько месяцев, так как потребляемый ток незначителен.

Современные закладные устройства, реализующие вышеописанные принципы, имеют различные габариты и форму. Самые маленькие из них напоминают пластмассовую рыболовную блесну. Отличительные особенности и технические характеристики некоторых типов аудиотранспондеров были описаны в п. 1.3.1.

Об их достаточно широком использовании говорит тот факт, что в 60-е годы американцы

жаловались на постоянное облучение ВЧ-сигналами их представительства в СССР с целью активизации встроенных резонаторов.
Кстати, использование подобных систем — достаточно вредное для здоровья дело: как для тех, кого подслушивают, так и для тех, кто подслушивает. Специалисты ЦРУ вынуждены были одевать специальные фартуки, предохраняющие важнейшие органы от влияния вредного излучения, когда сами облучали советские учреждения.
Применение полуактивных систем в рамках промышленного шпионажа — явление на Западе довольно редкое. На российском рынке подобные системы также пока не представлены и, видимо, не будут представлены еще несколько лет. Однако при дальнейшем совершенствовании противодействия техническим средствам разведки жизнь заставит заинтересованные организации настоятельно потребовать от производителей спецтехники выпуска полуактивных систем.
Кроме использования специальных средств, устанавливаемых на объекте, теоретически возможно зондирование отдельных радиотехнических устройств (телевизоров, приемников и т. д.), узлов бытовой техники, строительных конструкций. Однако на практике это крайне сложная задача, так как требуется перебрать множество вариантов по направлению излучения, частоте зондирующего сигнала, уровня, вида модуляции и т. п.
Перспективой развития подобных средств в радиодиапазоне является модернизация резонаторов с целью повышения индекса модуляции отраженного излучения и рациональный выбор частоты. Приоритетным направлением развития является и освоение более высокочастотных диапазонов (вплоть до миллиметровых волн). Можно предположить, что подобные резонаторы будут выполняться в виде отдельных узлов различного оборудования (кондиционеров, радиоприемников и т. д.) или элементов строительных конструкций. Об этом можно судить по широко известной истории строительства нового здания американского посольства в Москве. Обнаружив в 1982 году подслушивающие устройства, американцы прекратили строительство. Советская сторона в лице председателя КГБ В. Бакатина передала схемы размещения аппаратуры. Многие изделия удивили специалистов, при этом вершиной всего сочли саму конструкцию здания — «восьмиэтажного микрофона». Было объявлено, что направленное на него излучение соответствующей частоты модулируется некими специальными конструктивными элементами, которые способны улавливать звуковые колебания, возникающие при разговоре. Подозревали, что источник и приемник излучения находятся в стоящей через дорогу церкви Девяти мучеников Кизических. В разговорах американских экспертов она часто фигурировала как «храм Богородицы на телеметрии».

**Оптико-акустическая аппаратура перехвата речевой информации**

Наиболее перспективным направлением в области ВЧ-навязывания является использование лазерных микрофонов, первые образцы которых были приняты на вооружение американскими спецслужбами еще в 60-е годы.
Принцип работы этих устройств, получивших название лазерные системы акустической разведки (ЛСАР), заключается в следующем. Генерируемое лазерным передатчиком излучение (ВЧ-сигнал) распространяется через атмосферу, отражается от поверхности оконного стекла, модулируется при этом по закону акустического сигнала, также воздействующего на стекло, повторно преодолевает атмосферу и принимается фотоприемником, восстанавливающим разведываемый сигнал (рис. 1.3.43).
Сама модуляция зондирующего сигнала на нелинейном элементе, в качестве которого выступает оконное стекло, достаточно сложный физический процесс, который упрощенно может быть представлен в следующем виде:
1. Звуковая волна, генерируемая источником акустического сигнала, падая на границу раздела воздух—стекло, вызывает отклонения поверхности стекла от исходного положения. Отклонения приводят к дифракции света, отражающегося от этой границы.
Действительно, это заметно, например, при падении плоской монохроматической звуковой волны на плоскую границу раздела. Отклонения границы от стационарного состояния представляют собой бегущую вдоль стекла «поверхностную» волну с амплитудой, пропорциональной амплитуде смещений среды в поле звуковой волны, а длина А, этой поверхностной волны равна:

$$\lambda_п = \lambda_а / \sin\theta_3,$$

где $\theta_3$ — угол падения, и $\lambda_а$ — длина падающей акустической волны. 2. Отраженный от возмущенной поверхности свет содержит сдвинутые по частоте дифракционные

компоненты. Если поперечный размер падающего пучка лазерного излучения значительно превышают длину поверхностной волны, то отраженный свет представляет собой совокупность диф-

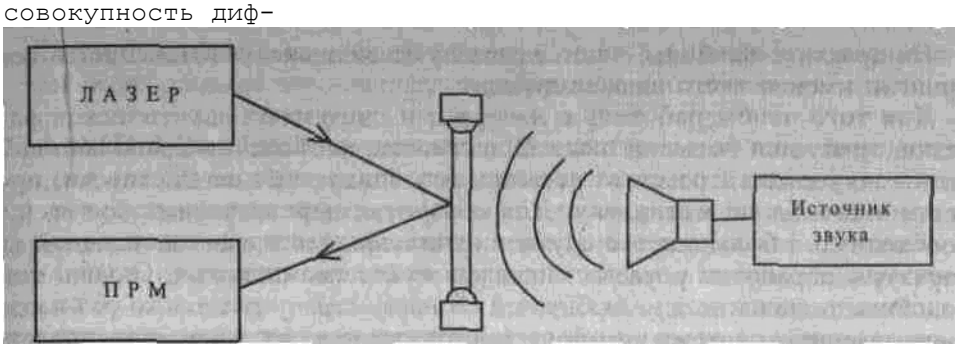



**Рис. 1.3.43. Принцип работы лазерного микрофона**

рагирующих пучков, распространяющихся по дискретным направлениям, определяемым из равенства:

$$\lambda_a k_c(\sin\theta_o - \sin\theta_m) = p,$$

где $\theta_o$ — угол падения исходного светового пучка, $k_c = 2\pi/\lambda_c$ — волновое число, $\lambda_c$ — длина световой волны.

В результате в отраженных пучках присутствуют три вида модуляции оптического излучения.

Во-первых, частотная модуляция, вызванная эффектом Доплера, вследствие колебательных движений оконного стекла под воздействием акустических сигналов.

При этом девиация частоты относительно центрального значения монохроматического излучения лазера подсветки имеет величину:

$$\Delta\omega = 2\pi/\lambda_a V_п,$$

где $V_п = C_з/\sin\theta_з$ - скорость распространения поверхностной волны, $C_з$ — скорость звука в среде.

Во-вторых, фазовая модуляция, вызванная наличием в отраженном сигнале как зеркально-отраженного, так и дифракционных компонентов.

Результат суперпозиции последних приводит к тому, что если поперечные размеры падающего оптического пучка малы по сравнению с длиной поверхностной волны, то в отраженном сигнале будет доминировать дифракционный пучок нулевого порядка. В этом случае и окажется, что фаза световой волны будет промодулирована во времени с частотой звукового сигнала.

В-третьих, амплитудная модуляция, вызванная колебаниями подсвечивающего пучка относительно направления зеркального (максимального) отражения.

Эти колебания вызваны также пространственным перемещением оконного стекла под воздействием акустического сигнала.

На практике наиболее часто используют системы, работающие на восприятии именно этого вида модуляции.

Для того чтобы работать с лазерными системами акустической разведки, требуется большой опыт. В частности, необходимо правильно выбрать точку съема, грамотно расположить аппаратуру на местности, провести тщательную юстировку. Для обработки перехваченных сообщений необходимо в большинстве случаев использование профессиональной аппаратуры обработки речевых сигналов на базе компьютера. Однако пока подобная техника не для любителей. В нашу страну несколько раз ввозились лазерные системы, но большинство из них так и не были проданы из-за высокой стоимости (от 10 до 130 тысяч $) и неподготовленности потенциальных пользователей, которые, кроме крика ворон, ничего не могли услышать.

Однако из печати известно, что лазерные микрофоны широко использовались против сотрудников советского (российского) посольства и консульств в США, подслушивались разговоры даже в семьях их сотрудников по месту жительства. Поэтому можно полагать, что так как опытные специалисты в состоянии скрытно применять подобные устройства, то весьма вероятно привлечение лазерных систем для решения задач конкурентной борьбы уже в ближайшем будущем.

На сегодняшний день создано целое семейство лазерных средств акустической разведки. Достижения в развитии лазерной техники позволили значительно улучшить технические характеристики и надежность работы данных систем разведки. Достаточно сказать, что появилась возможность дистанционной регистрации колебаний стекла с амплитудой вплоть до $10^{-14}$—$10^{-16}$ м, имеются сообщения о потенциальной возможности работы по объектам на расстояниях до 10 км, а наработка на отказ серийного гелий-неонового лазера составляет не менее 10 000 часов.

Примером современных ЛСАР могут служить устройства HP0150 фирмы «Хьюлет Паккард» и SIPE LASER 3-DA SUPER.

**HP0150** — лазерная система, обеспечивающая эффективное обнаружение, подслушивание и регистрацию разговоров, ведущихся в помещениях. Дальность его действия 1000 м. Устройство использует излучение гелий-неонового или полупроводникового лазера с длиной волны 0,63 мкм (что, кстати, является большим недостатком, так как пятно видно глазом, более современные системы работают в ближнем ИК-диапазоне). Прослушивание и перехват разговоров ведутся благодаря приему переотраженного сигнала от обычного оконного стекла, представляющего собой своеобразную мембрану, колеблющуюся со звуковой частотой и создающую фонограмму происходящего разговора. Приемник и передатчик выполнены раздельно. Кассетное устройство магнитной записи и специальный блок компенсации помех, а также треноги поставляются в комплекте устройства. Вся аппаратура размещена в небольшом чемодане. Электропитание — от батареи.

**SIPE LASER 3-DA SUPER** — данная модель состоит из источника излучения (гелий-неонового лазера), приемника этого излучения с блоком фильтрации шумов, двух пар головных телефонов, аккумулятора питания и штатива. Наводка лазерного излучения на оконное стекло нужного помещения осуществляется с помощью телескопического визира. Используется оптическая насадка, позволяющая изменять угол расходимости выходящего пучка, и система автоматического регулирования, задающая высокую стабильность параметров. Система обеспечивает съем речевой информации с хорошим качеством с оконных рам с двойными стеклами на расстоянии до 250 м.

Технические характеристики некоторых видов ЛСАР приведены в табл. 1.3.12, а внешний вид — на рис. 1.3.44.

На качество работы лазерных микрофонов существенно влияет большое количество различных факторов: погодные условия, уровни фоновых шумов, толщина и марка стекла, жесткость крепления стекла в раме, способ крепления рамы к стене, длина волны передатчика, точность юстировки аппаратуры, обработки сигнала, длина волны, уровень речи в помещении и т. д. В связи с этим сложно говорить о дальности перехвата информации вообще, можно рассчитать дальность съема информации из данного помещения данной аппаратурой в данных условиях. Кстати, немецкие специалисты даже в рекламных проспектах отмечают, что дальность действия лазерной аппаратуры от единиц до сотен метров.

Дальнейшее развитие лазерных систем, вероятнее всего, пойдет по пути уменьшения массогабаритных характеристик устройств за счет использования современных полупроводниковых лазеров, оптических устройств и средств первичной обработки сигналов с использованием ЭВМ.

В целом, о возможности применения вышеизложенных методов в интересах промышленного шпионажа можно сделать следующие выводы:

>- аппаратура, использующая принцип ВЧ-навязывания, — реальное средство несанкционированного получения речевой информации;

>- эффективность ее применения зависит от следующих факторов:

уровня речи;

>- расстояния от пункта контроля до объекта;

>- технических характеристик аппаратуры и средств вторичной обработки перехваченных сигналов;

>- погодных условий;

**Таблица 1.3.12. Лазерные системы акустической разведки**

Тип /Компонент /Тип прибора /Длина волны, мкм /Мощность, мВт /Фокусное расстояние, ММ (расходимость) /Габариты, мм (вес, кг) /Ток, мА/ Питание, В

STG-4510-LASER /Передатчик /Полупроводниковый /0.8...0.82 /5 /135 /— /150/12

/Приемник /PIN-диод /0,8...! / /500 /— /30/9

РК-1035-SS /Передатчик /Полупроводниковый /0,85 /5 /(0,5 мрад) /250х065 (1,6) /-/12 /Прием /Диод /0.8...1 / /135 /260х065 /-/3
/ник / / / / /(1,5) /
/Электронный блок /Фильтр, усилитель, магнитофон / / / /460х330х120 (3,2) /-/12
HKG GD-7800 - /Передатчик /Полупроводниковый /0,75...0,84 /5 /135 /— /-/12
/Приемник /PIN-диод /0,8...1 / /500 /Камуфлируется под стандартную камеру /-/12
Сапфир-040 /Передатчик /Полупроводниковый /0,83 /10 /- /565х400х180 (15) /-/12
/Приемник /- /Ближний ИК / /- /565х400х180 (15) /-/12.

степени подготовки лиц, использующих технические средства разведки;
>- применение подобной техники возможно только при тщательной предварительной подготовке;
>- использование аппаратуры ВЧ-навязывания в проводных каналах имеет хорошую перспективу из-за сравнительной простоты и дешевизны, известных методов;

**Рис. 1.3.44. Внешний вид лазерной системы акустической разведки**

>- использование лазерных систем в техническом плане не имеет серьезных проблем, и в обозримом будущем они станут обычным средством несанкционированного получения речевой информации не только спецслужб.

## 1.4. Оптические средства добывания конфиденциальной информации

### 1.4.1. Оптико-механические приборы

Зрение человека играет исключительно важную роль в познании окружающего мира, так как примерно 90 % получаемой информации приходится именно на зрение и только 10 % — на другие органы чувств. Интерес к секретам конкурентов, с долей иронии, также может рассматриваться как тяга к познанию. Отсюда и стремление определенной категории людей к прослушиванию конкурентов и получению некоторой зрительно осязаемой информации, например, о содержании интересующих документов и фотографий, о внешнем виде собеседников или передаваемых предметов во время конфиденциальной

встречи.
Однако мудрая природа, дав людям такой важный для восприятия окружающего мира прибор, существенно ограничила его возможности. Так, основными характеристиками человеческого глаза являются следующие:
>- мгновенное угловое поле зрения:
в горизонтальной плоскости составляет 65...95°;
в вертикальной плоскости — 60...72°;
>- расстояние наилучшего зрения — 250 мм;
>- время удержания взглядом изображения — 0,06 с;
>- область спектральной чувствительности лежит в диапазоне 0,37...0,72 мкм (рис. 1.4.1).
В соответствии с приведенной характеристикой максимальная восприимчивость для дневных условий соответствует темно-зеленому излучению с длиной волны X = 0,54 мкм (поэтому на зеленом цвете глаз отдыхает), а в сумеречное время — излучению с длиной волны X = 0,507 мкм — голубой цвет. Отсюда и известное выражение, что ночью все кошки серые.
Естественно и вечное стремление людей расширить границы своего зрения. Люди старались улучшить все характеристики зрения и создали огромное количество оптических приборов: для увеличения дальности наблюдения — зрительные трубы, бинокли и телескопы, для расширения области спектральной чувствительности — так называемые приборы ночного видения, для расширения поля зрения — системы телевизионного наблюдения, а для фиксации изображения — фотоаппараты, кино- и видеокамеры.

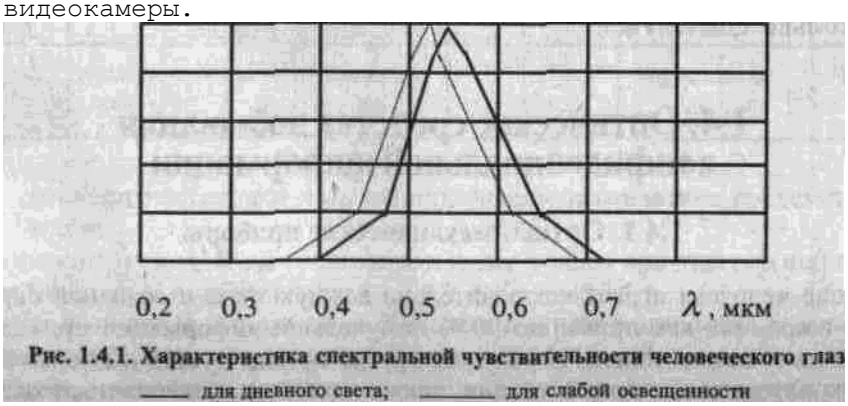
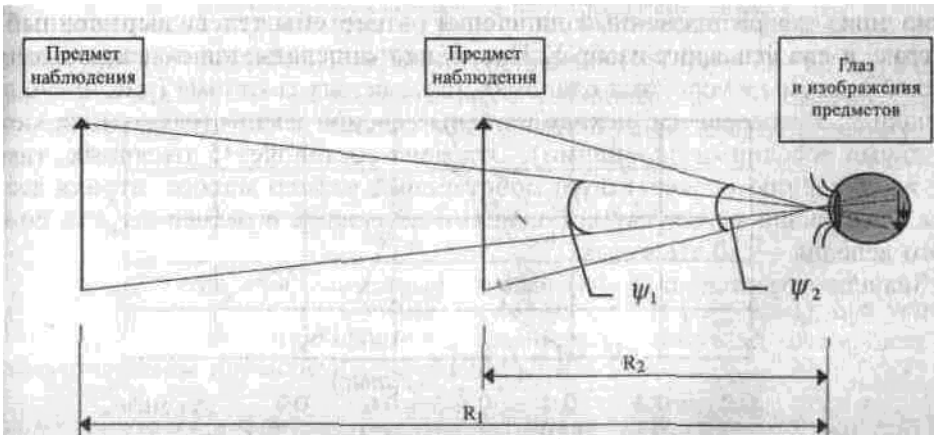


Рис. 1.4.1. Характеристика спектральной чувствительности человеческого глаз
—— для дневного света; _____ для слабой освещенности

Наиболее древними из перечисленных являются так называемые оптико-механические приборы, позволяющие зрительно приблизить удаленные предметы. Несмотря на свой «преклонный возраст» они до сих пор очень популярны и практически незаменимы для наблюдения за конкурентами с больших расстояний или из укрытий.
Принцип действия таких приборов основан на том свойстве, что один и тот же предмет виден под большим углом при меньшей "дальности (рис. 1.4.2).
Так, если невооруженным глазом предмет виден под углом $\psi_1$ , а оптическая система создает изображение, видимое под углом $\psi_2$ то видимое увеличение, или кратность увеличения определяется выражением:

$$\Gamma = \frac{\operatorname{tg}\psi_2}{\operatorname{tg}\psi_1} \approx \frac{\psi_2}{\psi_1}$$

В простейшем случае такая телескопическая система представляет собой двухкомпонентную афокальную систему, изображенную на. рис. 1.4.3. Чем больше ее длина, тем меньше угол $\psi_1$ ($\psi_1^{11} < \psi_1^{1}$ при $R^{11} > R^{1}$), а, следовательно, больше видимое увеличение Г. Так как величина угла $\psi_2$ согласована с размерами и воспринимающей способностью глаза и для нормальных условий составляет значение $\psi_2$ = 60°, то видимое увеличение оптико-механического прибора может быть оценено по диаметру входного отверстия объектива D, выраженного в миллиметрах:
Г[крат]=0,43D[мм].
(Хотя более Точное значение величины Г лежит в пределах от 0,2 до 0,75 D).




**Ряс. 1.4.2. Схема формирования воображения на сетчатке глаза: один и тот же предмет виден под большим углом ($\psi_2 > \psi_1$) при меньшей дальности ($R_2 < R_1$)**

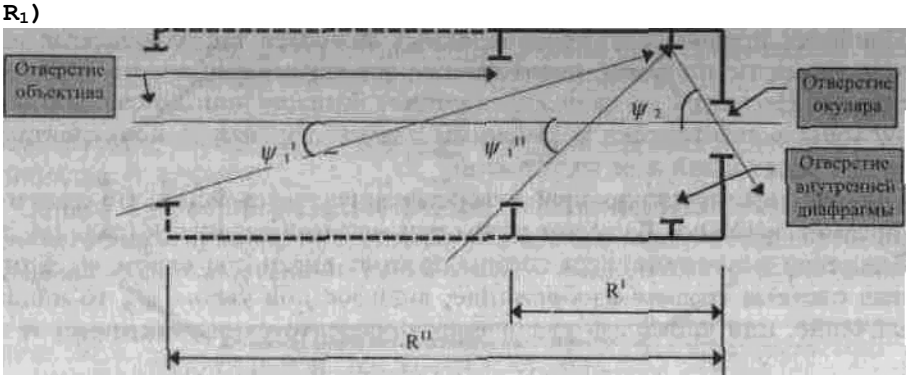



**Рис. 1.4.3. Двухкомпонентная телескопическая афокальная система**

Однако надо иметь в виду, что чем больше кратность увеличения, тем меньше мгновенное угловое поле зрения $\theta$, которое связано с величиной угла $\psi_2$, соотношением $\theta = \psi_2$,

В отверстия объектива и окуляра могут быть вставлены различные линзы (выпуклые, вогнутые, выпукло-вогнутые и др.), но для целей получения конфиденциальной информации лучше всего подходят двояковыпуклые линзы. Такая оптическая система известна под названием системы Кеплера, или астрономической трубы.

Достоинством системы Кеплера является то, что в плоскости изображения может быть установлена сетка (шкала). Она позволяет решать измерительные задачи по определению дальности до объекта наблюдения, в то время как другие оптические системы не могут быть использованы для этих целей.

Для того чтобы измерить расстояние R до объекта наблюдения, необходимо знать ориентировочный линейный размер объекта L, выраженный в метрах, и его угловой размер У. Последний определяется по шкале оптической системы в условных единицах, называемых тысячные (рис. 1.4.4, а). Величина У измеряется, исходя из цены деления шкалы (расстояния между двумя соседними делениями). Эта цена составляет 5 тысячных, такому же значению соответствует собственный размер малого штриха деления. Расстояние между двумя большими делениями и размер штриха большого деления — 19 тысячных.

Значение расстояния R (м) рассчитывается по формуле:

$$R\,[\text{м}] \approx L\,[\text{м}] \times \frac{1000}{У[тыс]}.$$

Так, например, на рис. 1.4.4, а представлен случай, когда в поле зрения оптической системы находятся человек и автомобиль.

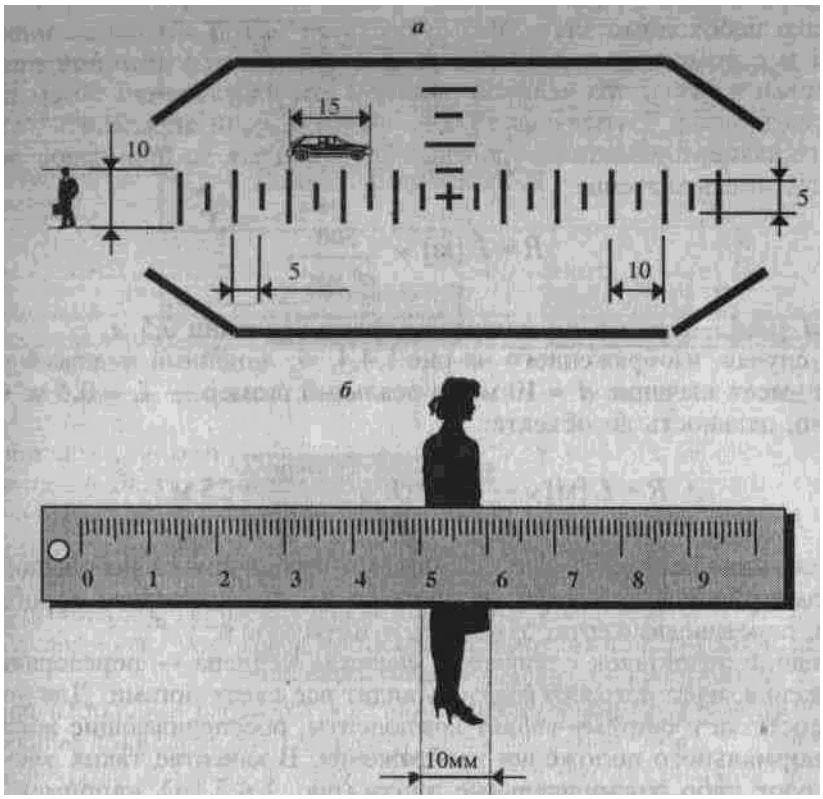



**Рис. 1.4.4. Определение расстояния до объекта:**
а — по шкале, установленной в оптической системе Кеплера;
б — с использованием линейки или других подручных средств

Известно, что средний рост человека составляет 1 м 70 см (L = 1,7 м), а его угловой размер для случая, изображенного на рисунке, У= 10 тысячных, таким образом расстояние от наблюдателя до человека составляет величину:

$$R \approx L\,[\text{м}]\frac{1000}{Y[\text{тыс}]} = 1{,}7 \times \frac{1000}{10} = 170\ \text{м}.$$

Длина другого объекта — автомобиля около 4,5 м (L = 4,5м), его угловой размер — У= 15 тысячных, следовательно дальность до автомобиля в рассметриваемом примере имеет значение:

$$R \approx L\,[\text{м}]\frac{1000}{Y[\text{тыс}]} = 4{,}5 \times \frac{1000}{15} = 300\ \text{м}.$$

Однако необходимо знать, что существует метод оценки дальности до объекта и с помощью подручных средств, например обычной линейки. Он основан на том, что угловой размер 1 мм на удалении 50 см от глаз составляет около 2 тысячных. Таким образом, если определить величину видимого размера объекта на удалении 0,5 м от глаз, то примерное расстояние будет иметь значение:

$$R \approx L\,[\text{м}] \times \frac{500}{d[\text{мм}]},$$

где d [мм] — видимый размер объекта на удалении 0,5 м. Для случая, изображенного на рис. 1.4.4, б, линейный видимый размер фигуры имеет значение d ≈ 10 мм, а реальный размер — L ≈ 0,5 м. Следовательно, дальность до объекта:

$$R \approx L\,[\text{м}] \times \frac{500}{d[\text{мм}]} = 0{,}5 \times \frac{500}{10} = 25\ \text{м}.$$

Вместо линейки может быть использован любой другой небольшой предмет геометрические размеры которого известны: спичечная коробка, карандаш, пластиковая карта, бумажная купюра и т. п.

Основной недостаток оптической системы Кеплера — переворачивание изображения, из-за чего наблюдатель видит все вверх ногами. Для устранения недостатка в систему вводят компоненты, обеспечивающие восстановление нормального положения изображения. В качестве таких элементов используют либо дополнительные линзы (рис. 1.4.5, а), например в подзорных трубах или телескопах, либо призмы (рис. 1.4.5, б), например в биноклях (рис. 1.4.6) или артиллерийских панорамах.

Для ведения скрытного наблюдения необходимо тщательно выбирать позицию с учетом местных условий и окружающего ландшафта. Для этих целей идеально подходят густая листва деревьев, различные строения, места складирования крупногабаритных предметов. Однако в ряде случаев оказывается затруднительно выбрать удобное место, и наблюдение приходится вести из-за угла, через препятствие и т. п. В этом случае хорошую услугу могут оказать упомянутые выше артиллерийские панорамы или другие оптические системы перископического типа, имеющие достаточно малые геометрические размеры входного объектива и изменяющие направление распространения оптических лучей.

Простейший перископ может быть изготовлен своими силами с использованием всего двух параллельно расположенных зеркал (рис. 1.4.7). Каркас для него также несложно сделать, применяя плотный картон, древесно-волокнистую плиту (ДВП), пластик.

Ведя скрытое наблюдение за объектом с помощью оптико-механического прибора, необходимо помнить о таком коварном демаскирующем

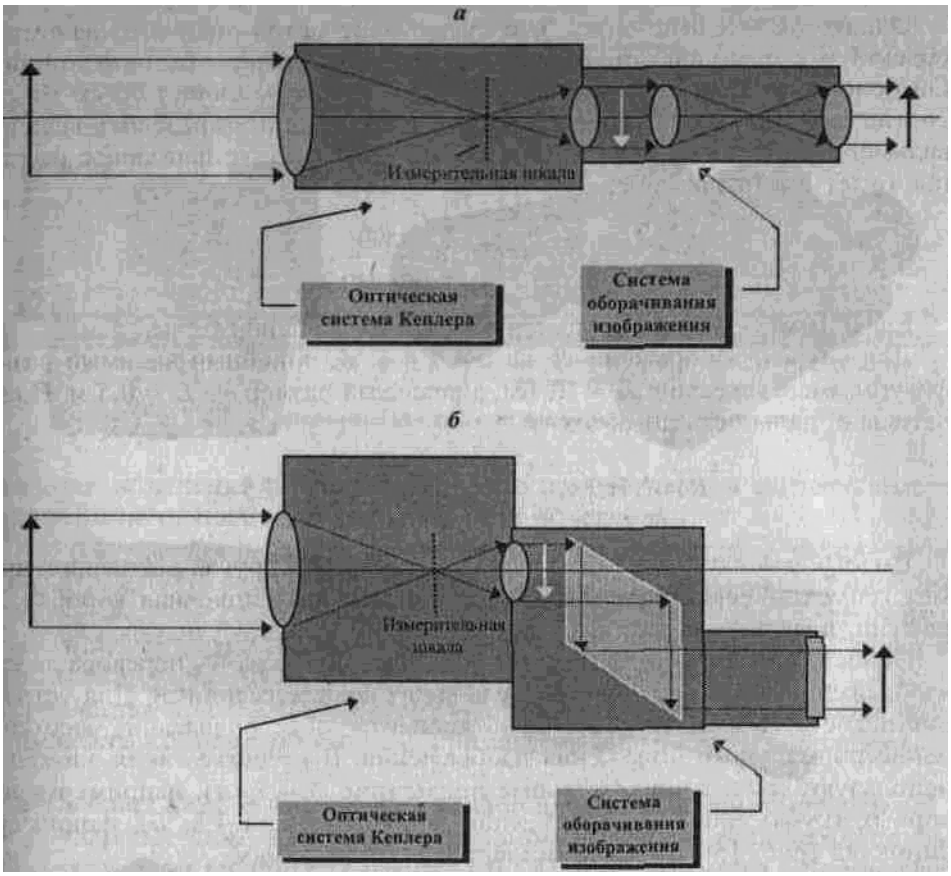



**Рис. 1.4.5. Восстановление нормального изображения в приборах с оптической системой Кеплера:**

а — зрительные трубы и телескопы; б — бинокли и артиллерийские панорамы

факторе, как солнечные блики на стекле вашей оптической системы, которые могут быть видны на расстоянии, достигающем нескольких километров. Чтобы не быть обнаруженным, необходимо выбирать позицию. Для наблюдения таким образом, чтобы прямые солнечные лучи не попадали на оптические стекла. Также надо знать, что существуют профессиональные оптические приборы, например военного назначения, с так называемой просветленной оптикой. Их отличительной особенностью является то, что на поверхность стекла входного объектива нанесена специальная пленка, толщина которой подобрана таким образом, чтобы лучи света, отраженные пленкой и стеклом, взаимно компенсировались,


**Рис. 1.4.6. Оптико-механические приборы для наблюдения за объектами с больших расстояний:**
а — полевой бинокль с 20-кратным увеличением; б — бинокль фирмы Pentax с 10-кратным увеличением; в — 8-кратный монокуляр фирмы Pentax с блендой; г — 8-кратные мини-монокуляры для скрытного наблюдения; д — 6-кратный бинокль фирмы Olympus

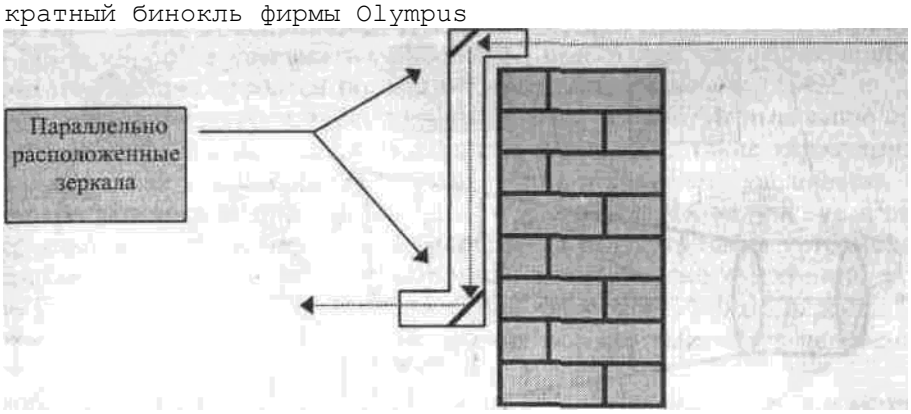



**Рис. 1.4.7. Перископическая система для скрытного наблюдения**
исключая появление бликов. Приборы с просветленной оптикой имеют

характерный темный цвет входных линз объектива.
Хорошей защитой от бликов может служить и бленда — специальный козырек в виде раструба, надеваемого на объектив оптического прибора. Она, во-первых, предотвращает попадание прямых солнечных лучей на вход объектива, а, во-вторых, существенно ослабляет переотражение лучей за счет специальной формы внутренней поверхности (рис. 1.4.6, в; 1.4.8).
В качестве примера современного оптико-механического прибора можно привести компактный бинокль британской фирмы BCB International.
**BCB Compact** 8x21 — оптический прибор для наблюдений, выполненный в ударопрочном и пыленепроницаемом корпусе с резиновым покрытием. При габаритных размерах 9,5x7x4 см его масса не превышает ;• 200 г. Линзы диаметром 21 мм имеют мгновенный угол поля зрения 7° и 8-кратное увеличение, что дает возможность наблюдать за участком местности шириной 130 м на дальности до 1000 м. Фокусировка и оптическая сила линз регулируются в зависимости от индивидуальных особенностей наблюдателя.

### 1.4.2. Приборы ночного видения

Рассмотренные выше оптико-механические приборы позволяют вести наблюдение при освещенности, близкой к нормальной (в светлое время суток), и при удовлетворительных погодных условиях (ясно или слабая дымка).
Естественно, что в жизни возникают ситуации, когда условия наблюдения затруднены — это вечернее или ночное время суток, чердаки, подвалы и т. п. В этих условиях неоценимую услугу могут оказать так называемые

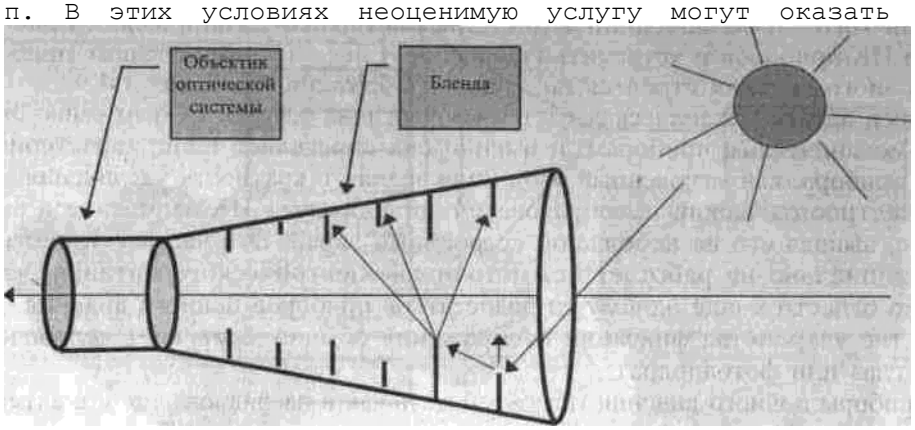



**Рис. 1.4.8. Устройство защиты оптической системы от солнечных бликов**

приборы ночного видения и тепловизоры, работающие в ближнем инфракрасном (ИК) диапазоне длин волн (X = 0,8...1 мкм).
Основное отличие между первыми и вторыми заключается в том, что тепловизоры реагируют на температурный контраст и поэтому принципиально не работают без охлаждения оптического приемника. Именно это обстоятельство говорит за то, что применение тепловизоров в интересах промышленного шпионажа маловероятно — преимущества при таком целевом назначении они дают незначительные, а по массогабаритным характеристикам существенно уступают приборам ночного видения. Так, на* пример, переносной тепловизор **Д-4** имеет габариты 195x212x260 мм и массу 3,4 кг, аналогичные характеристики и у прибора **ТМ-100.** Это, примерно, в 4—10 раз больше, чем у приборов ночного видения, а «легкий и компактный» тепловизионный датчик **V3900** (GEC-Masrconi Ltd — Великобритания), вообще имеет массу около 32 кг. Вследствие этого обстоятельства тепловизионные системы здесь рассматриваться не будут.
Главными достоинствами приборов ночного видения являются:
>- возможность наблюдения объекта в полной темноте или в условиях слабой освещенности;

>- меньшее по сравнению с видимой областью спектра затухание электромагнитных волн ИК-диапазона в осадках.

К недостаткам приборов следует отнести:

>- значительно худшую разрешающую способность, связанную с большой длиной волны (человека, например, можно опознать только по силуэту, так как черты лица не распознаются);

>- нечувствительность человеческого глаза к ИК-излучению.

Для того чтобы объединить достоинства оптико-механических приборов и ИК-приборов и устранить (уменьшить) недостатки последних приборы ночного видения строятся по схеме, изображенной на рис. 1.4.9.

Здесь оптико-механическая система аналогична рассмотренным выше оптико-механическим приборам, и именно она определяет такие характеристики прибора, как мгновенный угол поля зрения и кратность увеличения.

Электрооптический преобразователь преобразует ИК-излучение в видимое, выводя его на небольшой встроенный экран. Эта часть устройства принципиально не работает без источника электрического питания, что можно отнести к еще одному из недостатков приборов ночного видения. В качестве устройства фиксации изображения обычно выступает человеческий глаз или фотоаппарат.

Приборы ночного видения могут работать как в пассивном, так и в активном режиме. Пассивный режим применяется при наличии собственного излучения объекта наблюдения и в условиях слабого рассеянного излучения случайных искусственных или естественных источников, уровень которого превышает $10^{-5}$ лк (см. рис. 1.4.16). Активный режим используется в условиях полного отсутствия освещения. Он сопровождается применением источника подсветки объекта наблюдения. Таким источником может быть лазер, например полупроводниковый или на стекле с неодимом, или специальный ИК-прожектор. Прожекторы с мощностью излучения до 100—120 Вт функционируют, как правило, от автономных источников с напряжением питания 12 В. Диапазон расстояний, подсвечиваемых такими прожекторами, варьируется в диапазоне 10... 110 м, в зависимости от мощности источника и ширины луча, вид последнего формируется специальными насадками.

Технические характеристики ряда приборов ночного видения и источников подсветки приведены ниже, а внешний вид некоторых из них — на рис. 1.4.10 и 1.4.11 соответственно.

Устройства ночного видения

**РКЗОО** — прибор ночного видения, предназначенный для получения фотоснимков на стандартную пленку 35 мм. Применяется с объективами, имеющими фокусное расстояние 75 мм (светосила — F 1,4), фокусное расстояние — 135 мм (светосила — F 1,8) или 180 мм (светосила — F 2,8), угол зрения — 13,7°. Габариты: диаметр — 75 **мм**,

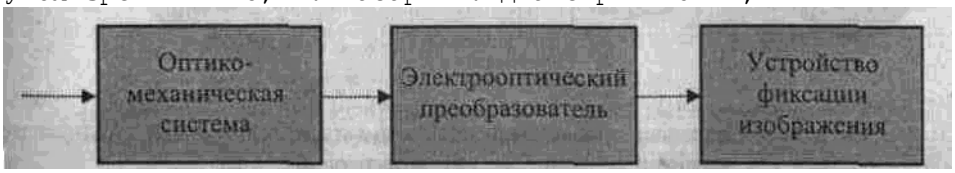



**Рис. 1.4.9. Структурная схема прибора ночного видения**

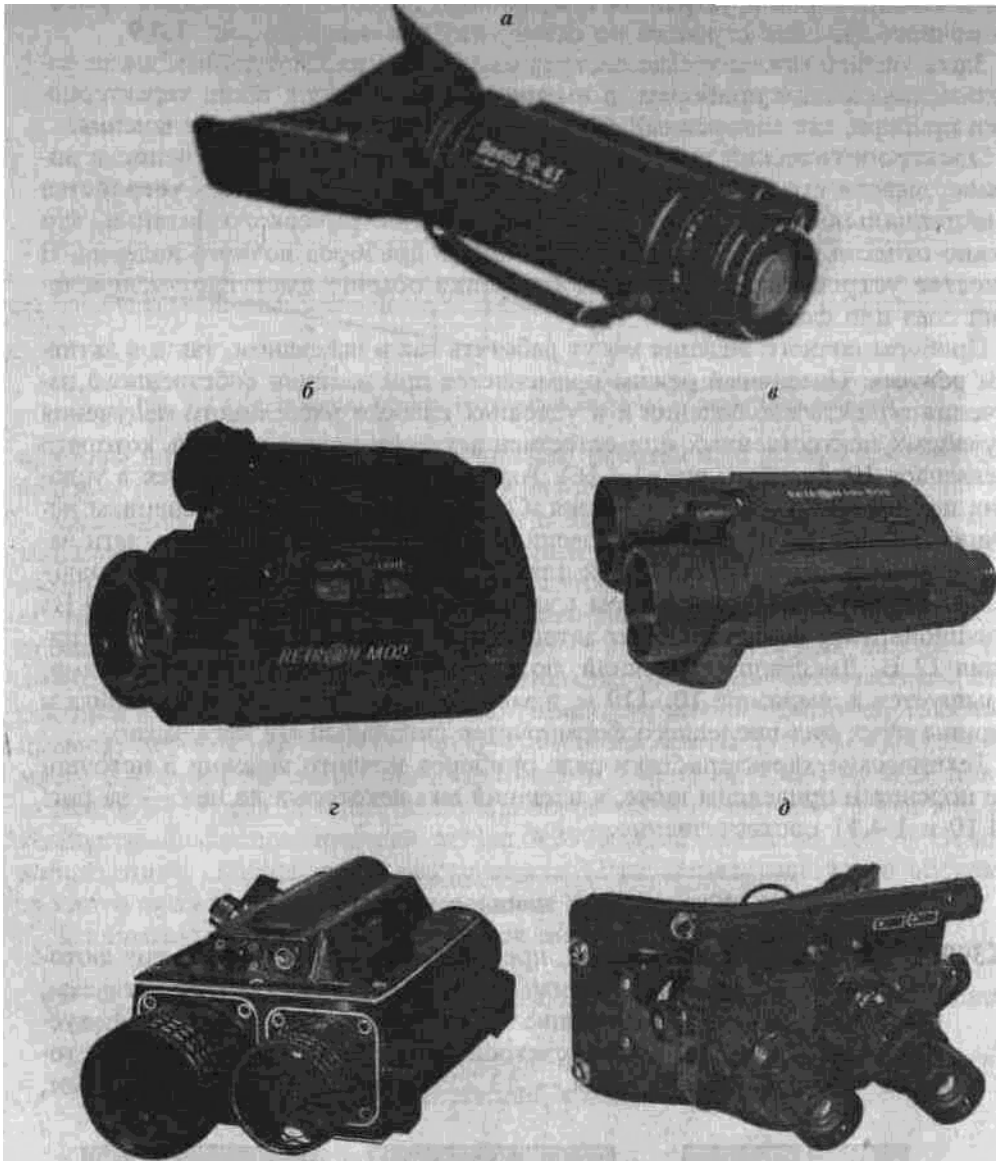



**Рис. 1.4.10. Приборы ночного видения:**
а — монокуляр DEDAL-0410; б — монокуляр RETRON RN-M02; в — бинокуляр RETRON RN-B03; г — активный ночной наблюдательный прибор с импульсной лазерной подсветкой; д — очки ночного видения OR 11


**Рис. 1.4.11. Средства подсветки объекта наблюдения ИК-лучамк**

а — лазерный источник излучения фирмы Dedal; б — инфракрасный лазерный осветительный прибор РК765; в - ИК-прожектор РК-325; г - ИК-прожекторы фирмы Dennari

длина — 350 мм; вес — 1,9 кг. Для фиксации изображения может комплексироваться с фотоаппаратом или видеокамерой.

**РК1260-S** — прибор ночного видения, предназначенный для получения фотоснимков объектов, находящихся на расстоянии до 10 км. Использует обычную фотопленку 35 мм.

**РК1245** — прибор для наблюдения удаленных объектов в условиях слабой освещенности (до $10^{-5}$ лк), фокусное расстояние объектива — 25 мм, светосила — F 1,4, угол зрения — 40°. Напряжение питания — 6,75 В, время непрерывной работы — 20 часов. Вес — 980 г. Выполнен в виде бинокля; **РК1245-S** — в виде шлем-маски.

**РК305** — прибор ночного видения активного типа, предназначенный для

наблюдения объектов в условиях полного отсутствия освещенности. Имеет объектив с фокусным расстоянием 135 мм и светосилой объектива F 2,8. ИК-прожектор имеет мощность 35 Вт и обеспечивает дальность наблюдения до 350 м. Собственный источник питания с напряжением 8 В обеспечивает время непрерывной работы 1,5 часа. Габариты прибора — 250x280x80 мм, вес — 1,3 кг.

**Dedal-220 —** монокулярный прибор ночного видения с угловым полем зрения прибора 28° в вертикальной и горизонтальной области. Диаметр объектива — 37 мм, светосила — F 1,0, кратность увеличения — 1,3. Усиление яркости изображения, создаваемое прибором, достигает 30 000. Габаритные размеры — 122x58x58, вес — 8 кг. Время непрерывной работы — 40 часов.

**Dedal-040** — прибор ночного видения, выпускаемый как в монокулярном, так и бинокулярном исполнении. Угловое поле зрения прибора в зависимости от конструктивного исполнения лежит в диапазоне 14°... 17°. Диаметр объектива — 85—100 мм, светосила — F 1,5...F 2,0, кратность увеличения — 1,9... 3,2. Усиление яркости изображения, создаваемое прибором, достигает 50 000. Габаритные размеры монокуляра — 210x76x93, бинокуляра — 325x76x103 мм, вес, соответственно, 1,12 и 1,52 кг. Время непрерывной работы — 50 часов.

**Spylux —** прибор ночного видения индивидуального применения. Заключен в прочный и компактный корпус, дает высококонтрастное изображение с хорошим разрешением при низких уровнях освещенности. Прибор имеет окуляр с регулированием фокусировки, кнопку включения— выключения и держатель объектива типа С с адаптером, дающим возможность менять объектив в соответствии с условиями наблюдения.

Стандартно прибор поставляется с объективом диаметром 75 мм и светосилой F 1,4. Масса прибора — 0,5 кг, напряжение питания — 2,0... 5,0 В, потребляемый ток — 16 мА.

**EEV Nite-Watch Plus** — самый компактный и легкий из приборов ночного видения фирмы EEV (Великобритания). Его масса (с объективом и батареей) составляет 330 г, габаритные размеры — диаметр 46x120 мм. Его легко спрятать в кармане. Прибор может комплексироваться через адаптеры с различными кино-, фото- и видеокамерами. Усиление яркости в приборе составляет не менее 20 000. Продолжительность непрерывной работы от одной батареи — 3 часа. Источник питания — литиевый элемент типа DL1/3N с напряжением 2,5...3,5 В. Потребляемый ток — 18 мА.

**EEV Black Watch** — прибор, специально разработанный для таких применений, как скрытое фотографирование и видеонаблюдение. Усиление яркости изображения, создаваемое прибором, достигает 2 000 000, что позволяет получать высококачественные фотографии в самых неблагоприятных условиях.

Источники ИК-подсветки

**PK765** — ИК-лазер с длиной волны 0,85 мкм и мощностью излучения в импульсе 180 мВт. Имеет форму цилиндра диаметром 65 мм и длиной 200 мм, напряжение питания — 12 В.

**IL-7/LR** — лазерный ИК-прибор подсветки, предназначенный для использования с приборами ночного видения при очень низких уровнях освещенности. Расходимость пучка регулируется от интенсивного карандашного пучка для точечной подсветки до пучка с расходимостью 40°. Масса прибора — 130 г с батареей электропитания, габариты — 63x50x20 мм. Длина волны излучения — 0,83 мкм, минимальная выходная мощность — 15 мВт. Электропитание — батарея литиевых элементов типа АА с напряжением 3,5 В. Продолжительность непрерывной работы — 5—20 часов.

**PK1420-S** — ИК-прожектор, предназначенный для подсветки фотографируемого объекта ИК-лучами. Дальность подсветки — 10—100 м. Диаметр прибора — 130 мм, длина — 240 мм, вес — 720 г.

**PK325** — ИК-прожектор, работающий в диапазоне длин волн 0,82...0,98 мкм.

Мощность — 110 Вт, дальность подсветки достигает 500 м. Напряжение питания — 220/110/12 В. Габариты: диаметр — 260 мм, длина — 200 мм. Вес — 2 кг.

Minilight 500 — миниатюрный ИК-излучатель на основе галогенной дихроичной лампы. В зависимости от модификации мощность лампы может быть 20 или 50 Вт. Напряжение питания — 12В. ИК-фильтр, предназначенный для задержки видимого света, пропускает излучение с длиной волны 0,84 мкм. Размеры источника излучения — 65х65х115 мм, масса — 350 г.

**AVS IR-1/48V** — светодиодный ИК-излучатель с длиной волны излучения 0,88 мкм. Минимальная дальность подсветки — 70 м, расходимость пучка — 30°, потребляемая мощность — 48 Вт. Питание осуществляется от источника постоянного напряжения 10—14 В. Габаритные размеры — 160х160х100 мм.

При ведении наблюдения с использованием приборов ночного видения необходимо учитывать следующие факторы:

>- оптимальная дальность ведения наблюдения составляет несколько десятков метров;

>- в поле зрения прибора не должно быть ярких источников света, так как их излучение может ослепить прибор или даже вывести из строя;

>- работать в активном режиме следует только в том случае, если точно известно, что объект наблюдения не использует приборы ночного видения, иначе вы будете им обнаружены.

### 1.4.3. Средства для проведения скрытой фотосъемки

Важным элементом промышленного шпионажа является получение документов, подтверждающих тот или иной вид деятельности конкурентов. При этом фотоматериалы могут быть незаменимы при решении задач документального подтверждения конфиденциальных встреч, факта посещения объектом наблюдения определенных мест, а также при анализе особенностей малознакомой, труднодоступной местности или при решении задач копирования текстовых документов, рисунков, схем, чертежей в условиях дефицита времени.

В зависимости от решаемых задач различают два вида фотосъемки: съемку объекта наблюдения и съемку документов (рис. 1.4.12).

Съемка объекта может осуществляться как с больших, так и с малых расстояний.

С больших расстояний фотографирование осуществляется из специальных укрытий, расположенных на крышах домов, чердаках, в автомобилях, в помещениях с окнами, выходящими на участок местности, представляю-


**Рис. 1.4.12. Виды скрытой фотосъемки**

щей определенный интерес. Высококачественные снимки при этом могут быть получены, если правильно решены следующие задачи:

>- выбор времени экспозиции и степени открытия диафрагмы;

>- подбор объектива;

>- определение точки производства фотосъемки.
Выбор времени экспозиции и степени открытия диафрагмы решаются достаточно просто при наличии фотоэкспонометра, определяющего величину светового потока, отраженного объектом и местными предметами. Прибор выдает несколько пар цифр, оптимальных для той чувствительности пленки, которая установлена в фотоаппарате. Например,
Время экспозиции, с /1/15 /1/30 /1/60 /1/125 /1/250 /1/500
Диафрагменное число, k /16 /11 /8 /5,6 /4 /2,8
любая комбинация из приведенных цифр (от 1/15 — 16 до 1/500 — 2,8) обеспечит один и тот же уровень светового потока, воздействующего на фотопленку. Однако конкретная пара должна выбираться, исходя из условий и задач съемки.
Так, при съемке движущихся объектов время экспозиции должно выбираться как можно меньше (например, 1/250 или 1/500 с) для того, чтобы уменьшить смазанность изображения, вызванную перемещением объекта в момент съемки. При этом, как видно из приведенной ниже таблицы, степень открытия диафрагмы будет максимальна (диафрагменное число 4 или 2,8, соответственно). В свою очередь, это приведет к уменьшению глубины резкости изображения. Например, при съемке объективом Гелиос-44М (табл. 1.4.1) с расстояния R = 10 м и k = 2,8 обеспечивается приемлемая рез-

**Таблица 1.4.1. Фотографические объективы**

Тип объектива /Диаметр апертуры, мм /Светосила /Фокусное расстояние (f), мм /Угол поля зрения, град
Гелиос-44М /29 /F2 /58 /31
Уран-9 /100 /F2,5 /250 /54
Уран-12 /200 /F2,5 /500 /38
Уран-24 /167/F3 /500 /46
Таир-16 /111 /F4,5 /500 /13
Таир-30 /67 /F4,5 /300 /.22
Телемар-2 /120 /F6,3 /750 /30
Телемар-17 /64 /F6.3 /400 /30

кость изображений только в интервале дальностей от 8 м до 15 м. Все предметы и объекты, находящиеся за пределами этого интервала будут выглядеть расплывчатыми (нечеткими). Глубина резкости изображения будет тем выше, чем больше значение диафрагмеиного числа 1с.
Важное значение для получения высококачественных снимков имеет правильный выбор объектива. Так, если необходимо получить детальный снимок объекта, находящегося на значительном расстоянии, то следует применять специальные длиннофокусные объективы, например, «Уран», «Таир» или «Телемар».
Они позволяют обеспечить хорошую опознаваемость изображенного объекта при съемке с расстояния, достигающего величины, примерно равной половине фокусного, расстояния оптической системы объектива, выраженного в метрах (R = 0,5f[м]). Так как объективы с фокусным расстоянием f= 400 мм и более оказываются достаточно громоздкими, то их часто строят по специальным многолинзовым схемам, позволяющим существенно уменьшить продольные габариты, примерно до значения l = 0,2f.
Однако рассмотренные выше объективы имеют малый угол поля зрения, а в ряде случаев возникает необходимость получения общего панорамного изображения какой-либо территории. Для этих целей следует применять специальные широкоугольные или сверхширокоугольные объективы с угловыми полями от 90 до 180°. Примеры таких объективов приведены в табл. 1.4.2.
Выбор типа фотоаппарата для осуществления вышеописанных видов съемки принципиального значения не имеет, лишь бы он позволял менять при

необходимости объективы. Тем не менее предпочтительней использовать аппараты с так называемыми зеркальными объективами, у которых визирование (наведение) осуществляется непосредственно через оптиче-

**Таблица 1.4.2. Широкоугольные фотографические объективы для панорамной фотосъемки**

Тип объектива /Диаметр апертуры, мм /Светосила /Фокусное расстояние (f), мм /Угол поля зрения, град
Русар-29 /8,8 /F9 /70 /120
Родина-26 /6,7 /F8,2 /55 /133
Орион-20 /- /F4,5 /- /130

скую систему объектива. Здесь незаменимым может оказаться фотоаппарат марки «Зенит» практически любой модификации, имеющий хорошие показатели по параметру качество—цена (рис. 1.4.13, л).

Определение точки съемки производится на основе комплексного анализа решаемой задачи, местных условий, возможностей аппаратуры и наличия естественных укрытий. Тем не менее, два следующих правила надо помнить всегда:

>- при проведении фотосъемки из помещения (или автомобиля) с закрытыми окнами стекла последних должны быть тщательно вымыты;

>- опасным демаскирующим признаком скрытой фотосъемки может быть появление солнечных бликов на стеклах объектива. Способы устранения бликов аналогичны тем, которые применяются при работе с оптико-механическими приборами.

Съемка объекта наблюдения может производиться и с малых расстояний, не превышающих нескольких метров. Естественно, что таким громоздким аппаратом, как «Зенит», в этих условиях можно снимать только под видом туриста, фоторепортера и т. п. Однако это не всегда безопасно и может насторожить объект наблюдения, тем более, что он может запомнить «фотографа».

В этом случае целесообразно маскировать аппарат под одеждой, в сумке, папке или в другом малогабаритном предмете, который можно, не вызывая подозрений, держать в руках (рис. 1.4.13, а...ж, к). Естественно, что и фотоаппарат должен отвечать решаемым задачам, поэтому он должен быть наделен следующими функциями:

**>-** иметь достаточно малые габариты и вес;
**>-** иметь автоматическую перемотку кадров после каждого снимка;
**>-** иметь автоматическую установку экспозиции;
**>-** иметь автоматическую наводку на резкость.

На удивление полно этим требованиям отвечают широко распространенные в продаже аппараты, получившие в просторечии название «мыльница» за внешнее сходство с вышеназванным предметом (рис. 1.4.13, о). Их массогабаритные характеристики позволяют легко маскировать аппарат. Благодаря встроенному электродвижку они обеспечивают производство повторных снимков с интервалом 2—3 с путем простого нажатия на кнопку пуска, а автоматическое наведение позволяет получать качественные снимки в интервале дальностей от 1,2 до 3,7 м. Тип фотоаппарата не имеет особого значения (Canon, Conica, Premier, Olympus...), единственное условие — наличие функции отключения встроенной в аппарат фотовспышки.

Съемку можно производить как через специально проделанные в предметах камуфляжа отверстия (в сумке, папке), так и непосредственно через ткань легкой одежды (хлопок, шелк, ситец...). Демаскирующими признаками описанной съемки являются достаточно громкий щелчок фотоспуска и характерный звук работы мотора при перемотке пленки.

Человеческая память обладает совершенно уникальным свойством со

временем забывать то, что в нее попадает. Эта защитная функция организма спасает наш мозг от переполнения ненужными знаниями, освобождая место для новой полезной информации. К сожалению, участи забывания не избегают и полезные сведения, что побудило в свое время людей изобрести письменность.

Записями в том или ином виде пользуются все, в том числе и ваши конкуренты, а получение этих записей или иных документов на бумажном носителе может иметь для вас стратегическое значение. Лучше всего, конечно, скрытно сделать копии этих документов, воспользовавшись, например сканером, факсом или ксероксом. Однако, вероятнее всего, этих удобных и полезных вещей в нужный момент под рукой у вас не окажется, и вы будете ограничены во времени. На выручку в такой ситуации может прийти старый, хорошо зарекомендовавший себя способ — репродукционная фотосъемка документов.

Для ее производства пригоден практически любой фотоаппарат, позволяющий установить специальный репродукционный объектив, предназначенный для копирования документов (рис. 1.4.13, з, п, р). Особенностью этих объективов является конструкция, позволяющая снимать документы с предельно малого расстояния (>1 см), в то время как обычные короткофокусные объективы ограничивают минимальную дальность величиной 0,5— 0,6 м, а при такой дистанции изображение получается мелким и труднораспознаваемым. Некоторые типы репродукционных объективов отечественного производства представлены в табл. 1.4.3.

Следует отметить, что для указанных целей хорошо подходит уже упомянутый фотоаппарат «Зенит», так как он имеет зеркальную систему визирования (что важно для получения хорошей резкости изображения) и позволяет копировать документы не только с использованием репродукционных объективов, но и с помощью обычных короткофокусных, например, «Гелиос-44М» (см. табл. 1.4.1). Однако в этом, случае необходимы специ-

**Таблица 1.4.3. Объективы для репродукционной фотосъемки**

Тип объектива /Диаметр апертуры, мм /Светосила /Фокусное расстояние, ММ /Угол поля зрения, град

Гелиос-91 /9 /F4,5 /40 /19
Эра-5 /7 /F3,5 /25 /26
Эра-7 /38 /F2,8 /105 /11
Эра-12 /31 /F4,0 /125 /16
Эра-13 /33 /F4,5 /150 /17
Эра-14 /48 /F2.8 /135 /12
Эра-15 /28 /F4,5 /125 /21
Маяк-1 /36 /F2,8 /100 /21

альные дополнительные кольца, устанавливаемые между фотоаппаратом и объективом.

К сожалению, выбор объектива не исчерпывает особенностей репродукционной съемки. Важное значение играет и подбор чувствительности фотопленки. С одной стороны, она должна быть достаточной для получения снимка в условиях естественной освещенности, а с другой — предельно малой. Так как, чем ниже чувствительность, тем меньше размер «зерна» фоточувствительного слоя и, следовательно, выше разрешение пленки (меньше размер фиксируемых деталей). Лучше всего для этих целей подходит фотопленка с чувствительностью по ГОСТу от 8 до 22 единиц.

Особо следует остановиться на совершенно новом типе аппаратов, которые еще достаточно экзотичны для российского рынка, но обладают удивительно

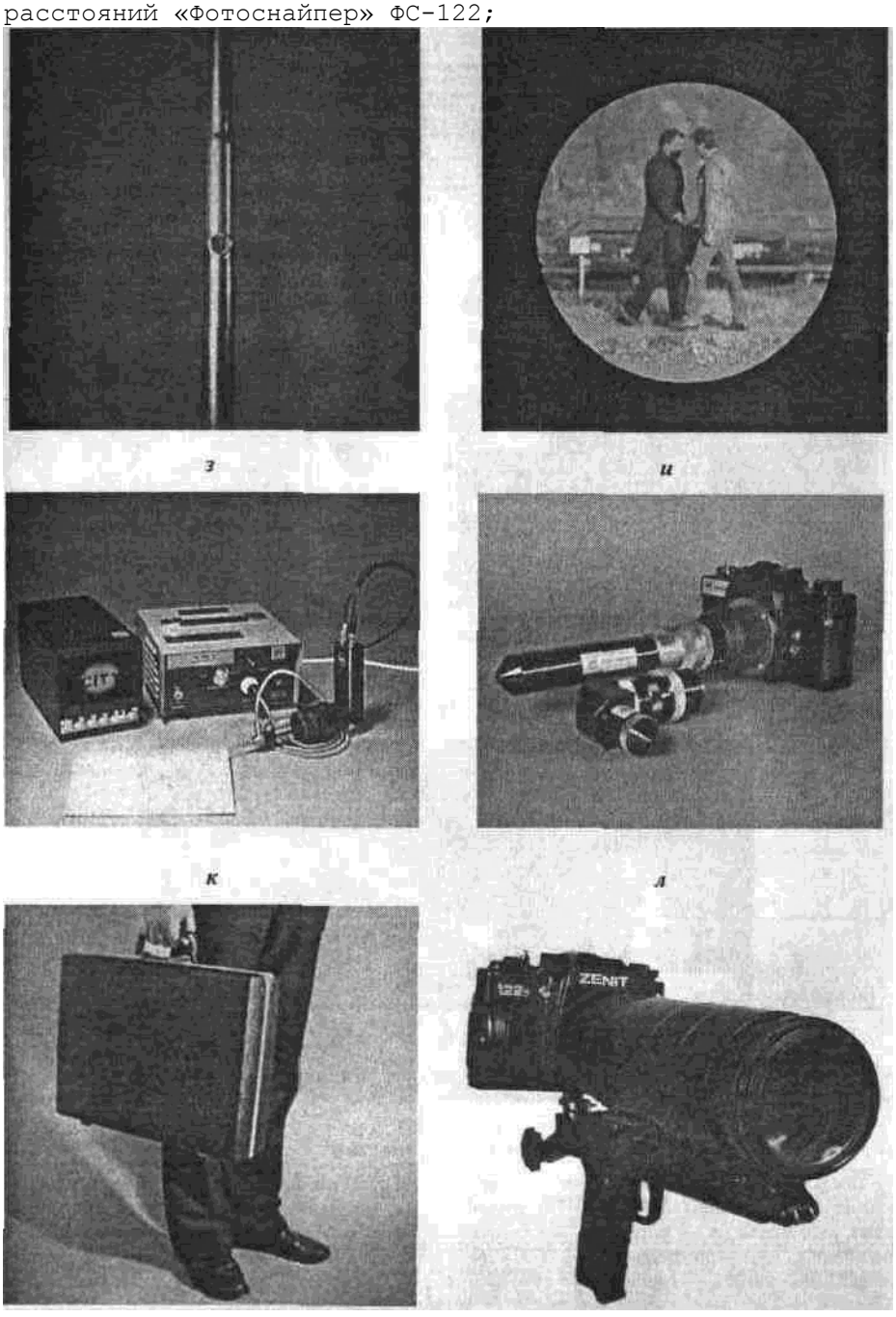
широкими возможностями. Это цифровые аппараты — digital cameras (рис. 1.4.13, м, н), фиксирующие изображение не на фотопленку, а в память, в виде, удобном для хранения, просмотра и обработки на персональном компьютере (форматы BMP, JPEG, TIFF). Объем внутренней памяти аппарата может достигать 4 MB. Этого вполне достаточно для производства примерно 190 снимков с нормальным уровнем разрешения. Перенос необходимых кадров на персональный компьютер осуществляется по специальному кабелю.

Скрытая съемка объекта наблюдения цифровым аппаратом в режиме автоматической установки параметров может осуществляться на дистанции **от** 0,6 м до °°, а оптимальная дальность лежит в пределах от 0,6 до 3,0 м. Частота производства снимков 0,5—5 с, и при этом полностью отсутствует демаскирующий фактор, связанный с работой мотора при перемотке пленки в камере.

Уникальность цифрового аппарата заключается и в том, что он пригоден для получения репродукционных снимков (пересъемки документов),


**Рис. 1.4.13. Фотоаппараты для негласной фиксации информации:**
а — наиболее широко используемая шпионская камера в период с начала 40-х по начало 90-х годов — аппарат-Minox; 6 — камера Ф-21, ее упрощенный вариант был в свободной продаже в СССР пол названием «Зенит МФ-1»; в — фотоаппарат «Киев-30», замаскированный в пачке из-под сигарет (также был в свободной продаже в СССР, естественно, без элементов камуфляжа);

г — фотоаппарат в ручных часах; д — фотоаппарат в зажигалке; е — аппарат в книге; ж — РК.1780 — фотоаппарат с объективом, встроенным в стандартную автомобильную антенну; з — РК1700 — устройство для чтения, фотографирования или снятия на видеокамеру текстов (писем), запечатанных в конверты; и — РК.1565 — специальный фотоаппарат с объективом Pin Hole; к — РК1690 — фотокамера с объективом Pin Hole, установленная в атташе-кейсе; л — фотоаппарат для съемки с больших расстояний «Фотоснайпер» ФС-122;



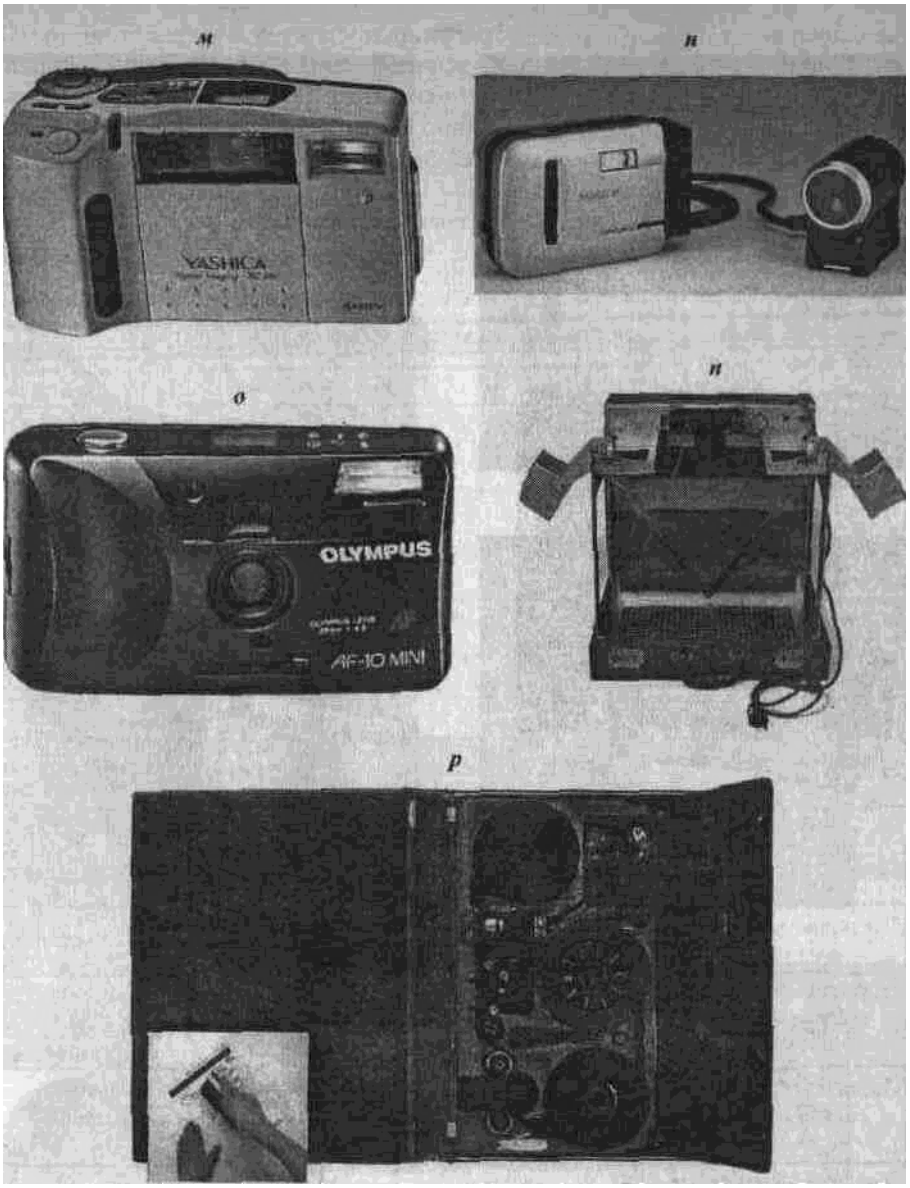



**Рис. 1.4.13. Окончание**

м — цифровая камера КС 600 фирмы Yashica; н — цифровая камера Dimage V фирмы Minolta; о — фотоаппарат-«мыльница» AF-10 MINI фирмы Olympus, идеально подходящий для скрытой съемки с малых расстояний; n — установка для репродукционной фотосъемки в атташе-кейсе с аппаратом фирмы Pentax; р — репродукционная фотокамера в записной книжке, работающая по принципу проката (сканирования) текста — специальные колесики на ребре переплета приводили в действие механизм камеры и включали встроенный источник света так как позволяет в режиме ручных регулировок снимать на расстоянии 0,01—0,6 м. Специальные мини-дисплеи, установленные на некоторых типах камер (например, Philips ESP-2), дают возможность контролировать качество получаемых изображений и оперативно менять параметры съемки.

Основные технические характеристики цифровых аппаратов фирм Philips и Panasonic приведены в табл. 1.4.4.

Более подробно технические характеристики ряда аппаратов, предназначенных для негласной фотосъемки, приведены ниже, а внешний вид некоторых из них — на рис. 1.4.13.

**Таблица 1.4.4. Основные характеристики цифровых аппаратов**

Основные характеристики /Типы аппаратов
/Philips ESP-2 /Panasonic KXL-600
Габариты, мм /128x34x72,6 /134x69x25
Вес, г /230 /182
Размер приемной матрицы, дюйм /1/4" /1/4"
Количество чувствительных элементов, (пикселей) /350 000 /360 000
Светосила объектива /F3,8 /F 2,8
Фокусное расстояние (/),мм /4 /5,2
Время срабатывания электронного затвора,с /1/5-1/8000 /1/15-1/4000
Интервал между снимками,с /5 /0,5- 1,0
Дальность съемки, м /0,6-∞ (стандартная) 0,6-3,0 (оптимальная) 0,01-0,6 (репродукционная) /1,0-∞ (стандартная) 0,5-1,0 (оптимальная) 0,13-0,15 (репродукционная)
Количество снимков, шт /25 (высокое разрешение) 50 (нормальное разрешение) 100 (экономичный режим) /48 (высокое разрешение) 192 (нормальное разрешение)
Наличие цвета в изображении /+ /+
Амплитуда видеосигнала при записи на компьютер, В /1 В на нагрузке 75 Ом /1 В на нагрузке 75 Ом
Напряжение питания,В /5 /3,3

**РК420** — специальная фотокамера, вмонтированная в электронные часы с жидкокристаллическим дисплеем (ЖКД), секундомером и будильником. Диаметр часов — 34 мм, толщина — 10 мм, вес — 70 г. Фотопленка представлена в виде кассеты из 7 кадров. В каждом кадре пленка имеет свою чувствительность в диапазоне от 15 DIN (ASA 25) до 22 DIN (ASA 125) для обеспечения съемки в различных условиях освещенности. Фиксированное фокусное расстояние обеспечивает диапазон дальностей производства фотосъемки от 1 м до бесконечности. Негатив диаметром 5,5 мм позволяет получать фотоснимки хорошего качества размером 9x9 см.

**РК415** — мини-фотокамера для репродукционной съемки и съемки на расстоянии на дальностях от 1м до бесконечности. Фиксированное фокусное расстояние объектива — 15 мм, светосила — F 5,6. Автоматическая регулировка времени экспозиции от 1/500 с до 8 с позволяет осуществлять фотосъемку в широком диапазоне уровня освещенности на пленку с чувствительностью от 15 DIN (ASA 25) до 27 DIN (ASA 400). Емкость кассеты — 12, 24 или 36 кадров. Размеры аппарата — 30x18x80 мм, вес — 50 г.

РК1570-SS — мини-фотокамера, закамуфлированная под зажигалку. Имеет объектив с фокусным расстоянием 12,5 мм и светосилой F 2,5. Позволяет использовать кассеты с 12, 24 и 36 кадрами, размер получаемого негатива — 8x11 мм. Фиксированное время экспозиции — 1/125 с. Размеры камеры — 26x16x110 мм, вес — 70.

**РК335-SS** — представляет из себя бинокль 9x30 мм с углом зрения 7° 10', совмещенный с фотоаппаратом, объектив которого имеет фокусное расстояние 300 мм и светосилу — F 5,6. Идеально подходит для наблюдения и фиксации событий. Габариты прибора — 208x140x129 мм, вес — 1,8 кг. Размер получаемого негатива — 24x36 мм.

**РК1565** — специальный фотоаппарат с объективом Pin Hole(СМ.Сноску 1) («игольное ушко»). Позволяет делать снимки через отверстия предельно мало-

___
Сноска 1. Pin Hole - дословно: отверстие, проколотое булавкой.

Изображение в аппарате с объективом Pin Hole формируется при помощи очень маленького отверстия без использования линз. Для такой оптики характерна большая глубина резкости, позволяющая фотографировать как близкие, так и удаленные объекты без дополнительной фокусировки. (Справедливости ради следует отметить, что этот оптический эффект известен людям со времен античной Греции и многие великие художники прошлого, включая Брунеллески, да Винчи, Дюрера и Рафаэля, использовали «камеру-обскуру» - помещение или большую коробку с маленьким отверстием на одной из стенок — для изучения законов перспективы.)

___
го диаметра без ухудшения качества изображения. Диаметр апертуры объектива — 3 мм, фокусное расстояние — 9 мм, угол зрения — 40°. Длина объектива — 120 мм, вес — 150 г;

**РК340-S** — автоматическая фотокамера, закамуфлированная под сумку-несессер, диапазон изменения времени экспозиции — от 1/750 до1 с. Светосила объектива — F 2,8, количество кадров — 110, вес — 360 г.

**РК1690** — фотокамера с объективом Pin Hole, установленная в атташе-кейсе. Установка параметров экспозиции — полностью автоматическая, размеры кадра — 24х36 мм. **РК1690-S** дополнительно снабжена радиоканалом дистанционного управления съемкой.

РК335 — камера, закамуфлированная под папку-скоросшиватель. Полностью автоматическая. Количество кадров — 36.

РК1780 — стандартная автомобильная антенна с 5-мм встроенным объективом, снабжена поворотным устройством вокруг вертикальной оси. Изображение фиксируется на фотоаппарат с автоматической регулировкой фокусного расстояния и времени экспозиции. **РК1780-S** — то же устройство, но снабженное видеокамерой **РК5105** для прямой видеозаписи наблюдаемого изображения либо передачи его на дальность до 3 км. Мощность передатчика видеосигнала — 1,5 или 10 Вт. **РК11930** или **РК193S** — специальные устройства для приема видеосигналов. Первый имеет размер экрана по диагонали — 23 мм, габариты — 83х167х49 мм, вес — 460 г и работает от автономного источника питания, второй имеет экран с диагональю 50 мм, габариты — 190х470х412 мм, вес — 4,4 кг и питается от сети 11Q/220 В.

**РК1700** — устройство для чтения, фотографирования или снятия на видеокамеру **РК5105** текстов (писем), запечатанных в конверты. Представляет из себя специальный эндоскоп длиной 170 мм с фиксированным фокусным расстоянием и углом зрения 70°, его диаметр равен 1,7 мм. Устройство вводится в нераспечатанный конверт и перемещается вдоль текста, который можно прочесть, например, на экране монитора (23 см по диагонали). В устройство входит и специальный источник подсветки **РК1765 с** напряжением питания 220 В и мощностью 150 Вт.

**РК1705 —** прибор для прямого наблюдения, фотографирования или снятия на видеокамеру РК5105. Жесткий эндоскоп длиной 245 мм, диаметром 6 мм вставляется в отверстие в стене. Вес прибора 320 г, угол зрения 80°. Дальность наблюдения — от 0,5 м до бесконечности.

Модель **РК1780-S** содержит встроенный аудиомикрофон и усилитель с коэффициентом усиления 20 000 раз, напряжением питания 9 В и частотным диапазоном 300—3000 Гц. Размеры усилителя — 54х80х20 мм. Он позволяет прослушивать помещение с помощью головных телефонов.

**1.4.4. Технические средства получения видеоинформации**

Наиболее совершенным способом получения конфиденциальной информации является скрытое телевизионное или видеонаблюдение. Применение специальных миниатюрных камер позволяет сделать это наблюдение абсолютно незаметным, информативным и безопасным.

Однако по своей структуре телевизионные камеры более сложны, чем рассмотренные выше приборы ночного видения. Это связано с

необходимостью разложения получаемого изображения на составные части для их передачи к месту регистрации и последующего восстановления передаваемого изображения (дословно телевидение — это видение на расстоянии). В общем случае структурная схема телевизионной камеры имеет вид, показанный на рис. 1.4.14.

Здесь объектив играет такую же роль, как и в рассмотренных выше оптических приборах, но конструкция его может быть сложнее из-за необходимости решения задачи автоматической регулировки диафрагмы в зависимости от уровня освещенности объекта наблюдения (рис. 1.4.15). Характеристики некоторых современных телевизионных оптических систем приведены в табл. 1.4.5.

Фотоприемник предназначен для преобразования светового потока, отраженного объектом в электрические сигналы. В подавляющем большин-

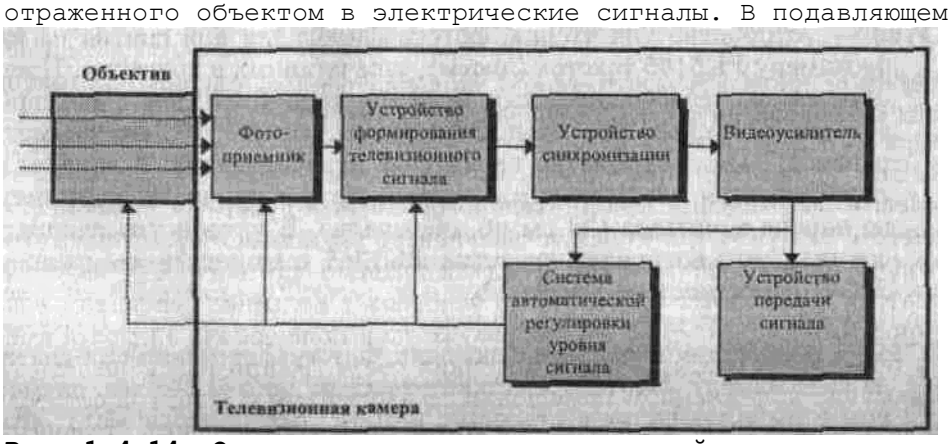



**Рис. 1.4.14. Основные элементы телевизионной камеры**

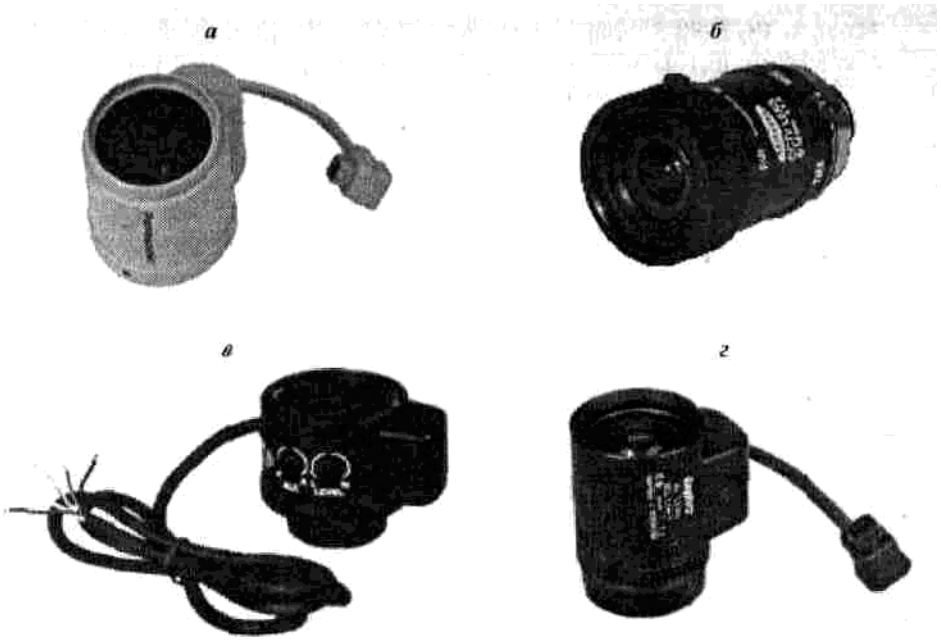



**Рис. 1.4.15. Объективы телевизионных и видеокамер:**
а — Panasonic WVLA4AR5C3A; б — Samsung SLM-604CN; в — Samsung SLA-064C; г — Sanyo VCL-CS42Y

стве современных телевизионных камер для этих целей используют так называемые ПЗС-матрицы.

Устройство формирования сигнала, устройство синхронизации и видеоусилитель обеспечивают формирование полного телевизионного сигнала

заданной структуры и амплитуды.
Система автоматической регулировки уровня сигнала, управляя электронной диафрагмой объектива (АРД), временем накопления электронного заряда в ПЗС-матрице (временем срабатывания электронного затвора) и параметрами усиления, поддерживает выходной видеосигнал в заданных пределах при изменении условий освещенности.
Некоторые камеры дополнительно оснащены функцией компенсации заднего света (КЗС), которая устанавливает указанные параметры по некоторому фрагменту изображения (как правило, по центру). Она может оказаться незаменима при работе в условиях с большим перепадом освещенности или при съемке в условиях, когда в поле зрения аппарата вместе с объектом попадает яркий источник света. Например, если ведется наблюдение в затененном помещении за входящими с улицы посетителями, то в яркий солнечный день на экране видеоконтрольного устройства вместо четкого изображения входящего может оказаться только темный

**Таблица 1.4.5. Характеристики некоторых типов современных телевизионных объективов**

Тип объектива /Диаметр апертуры, ММ /Светосила /Фокусное расстояние, ММ /Угол поля зрения, град /Установочная резьба /Примечание
iVi-1,0 /14 /F1.8 /3,6 /110 /M12 /
iVi-2,0 /13 /Pl,8 /4.1 /90 /M12 /
iVi-3,0 /3.4 /F 1,8 /6,6 /50 /M12 /
iVi-4.0 /4,6 /Fl,6 /7,7 /40 /M12 /
iVi-7,0 /1.2 /F2,8 /3,5 /110 /— /
iVi-10 /6,5 /F2.8 /19,5 /16 / /Вынос зрачка(СМ.Сноску 1)— 12.5 мм
HS3 166-X /3,7 /F 1,6-64 /— /— /cs(СМ.Сноску 2) /АРД(СМ.Сноску 3)
HS4 166-X /4.2 /F 1,6-64 /— /— /cs /АРД
HS614HX /2,6 /F 1,6-300 /— /— /cs /АРД

силуэт. Достоинство функции КЗ С заключается в том, что она настраивает камеру именно по слабоосвещенному объекту в центре, обеспечивая его четкое изображение.
Устройство передачи сигнала — это радиопередатчик, аналогичный применяемым в радиозакладных устройствах, полупроводниковый лазер или электрический кабель в зависимости от способа применения телевизионной системы наблюдения.
Современные телевизионные камеры характеризуются большим числом различных параметров, однако, с точки зрения скрытого наблюдения, наибольший интерес представляют следующие:

___
Сноска 1. Объективы с вынесенным зрачком могут работать через отверстия, диаметр которых меньше диаметра апертуры зрачка, например, при скрытой установке видеокамеры в стене.
Сноска 2. В ряде стран существуют два типа стандартных конструкций узлов крепления объективов: тип С и тип CS. Тип С имеет резьбу 2,54x0,8 и расстояние до опорной плоскости ПЗС-матрицы 17,5 мм, тип CS имеет резьбу 2,54x0,8 и расстояние до опорной плоскости матрицы 12,5 мм. Объективы с узлом крепления типа С нельзя заменять типом CS, так как матрица окажется не в фокусе объектива и изображение получится нечетким. В то же время объективы с CS можно использовать вместо объективов типа С при наличии специального адаптера (переходного кольца).
Сноска 3. АРД — автоматическая регулировка диафрагмы, позволяет поддерживать постоянный уровень освещенности ПЗС-матрицы при изменяющихся внешних условиях.

___
>- мгновенный угол поля зрения;
>- разрешающая способность;
>- чувствительность телевизионной камеры.

Мгновенный угол поля зрения полностью определяется конструкцией оптической системы. Его значения для различных типов объективов приведены в табл. 1.4.5.

Разрешающая способность включает в себя два понятия: разрешающую способность объектива и разрешающую способность фотоприемника.

Разрешающая способность объектива, $\Delta l$ — это тот предел, к которому стремится любая система фиксации изображения. Она зависит от диаметра D, входного зрачка объектива и расстояния R от телекамеры до объекта наблюдения и соответствует минимальному линейному разносу двух точек на объекте, при котором они воспринимаются еще раздельно. Значение $\Delta l$, может быть определено из соотношения:

$$\Delta \ell \approx 1{,}22 \frac{\lambda}{D} R .$$

Здесь l — среднее значение длины волны оптического излучения (для видимой области спектра $\lambda \approx 0{,}54$ мкм, а для ИК-области — $\lambda \approx 0{,}9$ мкм).

Разрешающая способность фотоприемника хуже (больше) разрешающей способности объектива, поэтому ее величина и определяет разрешение телевизионной системы в целом. Она зависит от числа чувствительных элементов ПЗС-матрицы (пикселей), из выходных сигналов которых складывается изображение. Их число обычно лежит в пределах от 270 000 до 440 000. Чем больше число пикселей в матрице, тем больше дискретных точек образует изображение, тем выше его четкость и качество. Однако на практике часто пользуются не понятием «количество чувствительных элементов матрицы», а апеллируют к однозначно связанной с ней характеристике — максимальному количеству переходов от черного к белому и обратно. Она называется числом телевизионных линий и указывается, как правило, только по горизонтали.

Некоторые фирмы в технических характеристиках на свои телевизионные камеры дополнительно указывают размер матрицы оптического приемника. В большинстве представляемых на российском рынке камерах используются датчики изображения (матрицы) с размером: 1 дюйм; 2/3 дюйма; 1/2 дюйма; 1/3 Дюйма; 1/4 дюйма. Последние, как правило, применяются только в сверхминиатюрных камерах, используемых для скрытого наблюдения.

По чувствительности к уровню освещенности телевизионные камеры делятся на пять классов:

≈ I — камеры, которые могут работать только при нормальном дневном освещении (при уровне освещенности E=50 лк);

>• II — камеры, способные работать при низкой освещенности вплоть до наступления сумерек (E ≈ 4 лк).

>• III — камеры, предназначенные для работы при лунном свете, соответствующем уровню освещенности от четверти луны в безоблачную ночь (E ≈ 0,1...0,4 лк).

>• IV — камеры, способные работать при уровне освещенности, создаваемой безлунным звездным небом в безоблачную ночь (E ≈ 0,0007...0,002 лк).

>• V — камеры, предназначенные для работы с дополнительными источниками ИК-излучения в условиях полного отсутствия видимого излучения.

Следует еще раз обратить внимание на то, что телевизионные камеры, предназначенные для работы в условиях низкого уровня освещенности отличаются от приборов ночного видения более сложным представлением сигнала. Это связано с необходимостью передачи его на расстояние, в то время как приборы ночного видения позволяют только фиксировать

информацию, например, глазом или фотоаппаратом.
Выбирая класс телевизионной камеры, необходимо знать, что чувствительность Е ее телевизионного приемника должна отвечать условию:

**E ≥EoxRxK,**

где Ео — общий уровень освещенности в зоне нахождения объекта наблюдения [лк]; R — коэффициент отражения объекта наблюдения; К — коэффициент пропускания объектива камеры. Значения параметров R и К приведены в табл. 1.4.6 и 1.4.7, соответственно, а типовая зависимость уровня освещенности Ео от времени суток и состояния атмосферы — на рис. 1.4.16.
Для скрытой телевизионной (видео-) съемки обычно используют малогабаритные камеры (рис. 1.4.17), которые могут быть выполнены как в обыч-

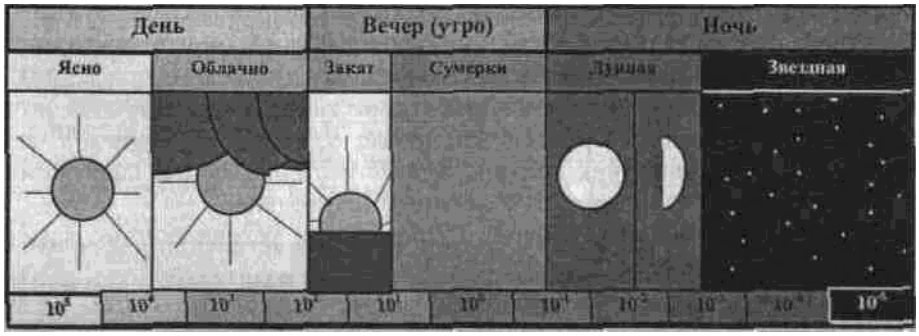



**Рис. 1.4.16. Типовая зависимость уровня освещенности Ео [лк] от времени суток и состояния атмосферы**

ном, так и закамуфлированном исполнении (например, в виде дверного «глазка»); существует целое семейство бескорпусных видеокамер. Для осуществления наблюдения вышеперечисленные устройства устанавливают в элементы конструкций зданий, предметы интерьера или прячут под одежду.
Так например, телевизионная камера **JT-241s** штатно оснащается следующими предметами камуфляжа:
>• элементы интерьера: картина, мебель, цветочная ваза, статуэтка, светильник, электророзетка;
>• одежда и ее элементы: куртка, костюм, заколка для галстука, пуговица, пряжка ремня;
>• носимые предметы: кейс, сумка, радиоприемник, магнитофон.

**Таблица 1.4.6. Коэффициенты отражения различных типов поверхности**

Отражающая поверхность /Коэффициент отражения
Кожа человека /0,15—0,25
Ткань серого цвета /0,2—0,6
Ткань желто-коричневого цвета /0,3—0,4
Ткань ярко-голубого цвета /0,35—0,6
Ткань ярко-зеленого цвета /0,5—0,75
Ткань желтого цвета /0,6—0,75
Ткань цвета слоновой кости /0,75—0,8
Ткань грязно-белого цвета /0,75—0,85
Ткань белого цвета /0,8—0,9

**Таблица 1.4.7. Коэффициенты пропускания объективов телевизионных камер**

Светосила объектива /Относительное отверстие объектива /Коэффициент пропускания
F 0,8 /1: 0,8 /0,31
F 0,95 /1:0,95 /0,2
F 1,2 /1: 1,2 /0,14
F 1,4 /1: 1.4 /0.1

F 2,0 /1: 2.0 /0,05
F 2,8 /1: 2,8 /0,025
F 4,0 /1: 4,0 /0,0125
F 5,6 /1: 5,6 /0,00625
F 8,0 /1% 8,0 /0,003125

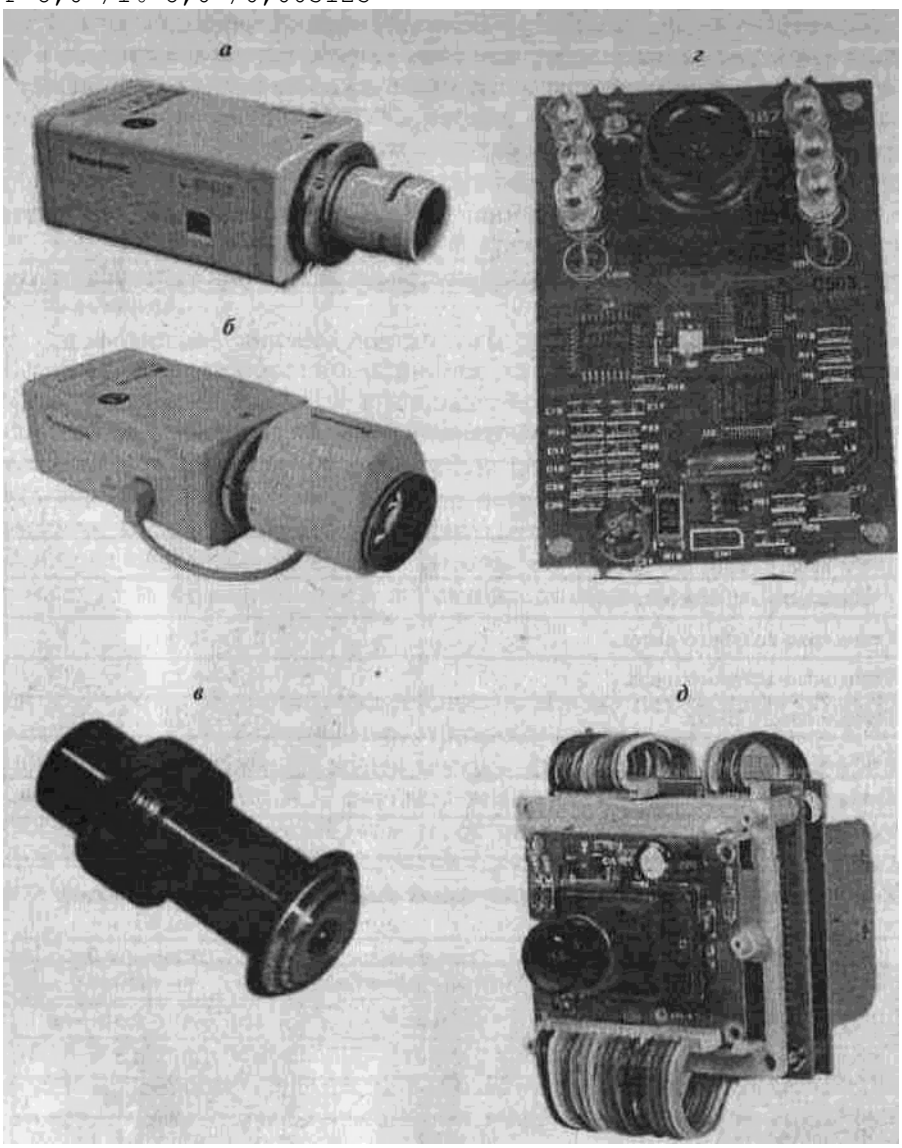



**Рис. 1.4.17. Малогабаритные камеры для скрытого наблюдения:**
а — Panasonic WV-CP410; б — Panasonic WV-BP120; в — видеокамера-глазок МВК-17(А), снабженная звуковым каналом; г — бескорпусная камера С-503; д — бескорпусная камера С-770

**ПРОМЫШЛЕННЫЙ ШПИОНАЖ**

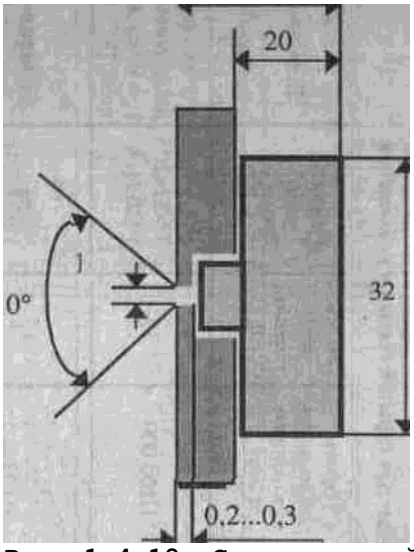



**Рис. 1.4.18. Схема скрытой установки телевизионной камеры типа JT-241s**

Один из вариантов скрытой установки этой камеры за плоским укрытием показан на рис. 1.4.18.

Важным достоинством указанной камеры является наличие специального передатчика телевизионного сигнала **JR-500,** позволяющего передавать изображение и звук на расстояние до 500 м. Передатчик работает в диапазоне дециметровых волн, имеет габариты 120x120x25 мм и массу 200 г. Питание — от элемента с напряжением 12 В. Предусмотрено закрытие передаваемой информации.

Дополнительно камера оснащается выносным проводным микрофоном **JM-004** и оптико-волоконными жгутами для вынесения объектива, прожектором инфракрасной подсветки, диктофоном и видеомагнитофоном. В зависимости от комплектации камера может использоваться как носимое средство либо как закладное устройство.

С целью увеличения времени автономного функционирования в качестве закладки телевизионная камера может оснащаться приемником сигналов дистанционного управления. Время непрерывной работы в зависимости от комплектации и режима функционирования изменяется в пределах от 30 минут до 30 часов.

Для приема телевизионных и аудиосигналов от передатчика JR-500 применяется специальный приемник JD-500, обеспечивающий уверенный прием на указанной дальности — до 500 м. Основные технические характеристики телевизионной камеры JT-241s, а также некоторых других приведены в табл. 1.4.8.

**Таблица 1.4.8. Телевизионные и видеокамеры, предназначенные для скрытой съемки и наблюдения**

Тип камеры (фирма - страна производитель) /Минимальная освещенность, лк /Горизонтальное разрешение, телевизионных линий /Размер чувствительного элемента /Параметры объектива /Время срабатывания электронного затвора, с /Напряжение питания, В /Габариты, ММ (масса, г) /Примечание

1 /2 /3 /4 /5 /6 /7 /8 /9

JT-241S (Тайвань) /0,04 /400 /1/3" /D= 0,3-1,2 мм; F 2,8; 9=110° /1/100000 /12 /32x32x20 (20 г) /Аудиоканал; дистанционное управление (ДУ).

MYTHOS (Bisset -Франция, Южная Корея) /0,3 /380 /1/3" /0=4 мм; Fl,6 /— /12 /— /Аудиоканал

ПКС-504С (ЭВС - Россия) /0,08 /380 /1/3" /F 1,4; CS /1/50-1/10000 /— /— /—

ПКС-504Н (ЭВС - Россия) /0,005 /380 /1/3" /F1.4; CS /1/50-1/10000 /— /— /—

ПКС-754СМ (ЭВС - Россия) /0,05 /380 /1/3" /Fl,4; CS /— /— /— /Аудиоканал

ДО-1 (ЭВС - Россия) /0,005 /380 /1/3" /Fl,4; θ=90° CS /— /— /— /АРД

FC-65 (Computar -Япония) /0,3 /380 /1/3" /Fl,4 /1/50-1/100000 /12 /55x40x102 /—

XC-41 (Computar - Япония) /10 /320 /1/3" /0=4 мм; F2.0 /— /12 /55x60x30 /Бескорпусная, цветное изображение

WAT-308 (Watec -Япония) /0,05 /350 /1/3" /F 1,4; CS /1/50-1/100 000 /,12 /41x41x43 /—

WAT-502A (Watec -Япония) /0,1 /400 /1/3" /F1.2; CS - /1/50 -1/100 000 /9 /31,5x30,5x54 /—

WAT-660D-G3,8 (Watec -Япония) /0,8 /380 /1/4" /D = 3,8 мм; F2,0; θ=51 /1/100000 /9 /30x30x30 /Бескорпусная

WAT-660D-P3,7 (Watec - Япония) /4 /380 /1/4" /D=3,7 мм; F4,5; 0=52° /1/100000 /9 /30x30x16 /Бескорпусная, вынесенный объектив

WAT-704R-P3,7 (Watec - Япония) /0,8 /380 /1/4" /D=3,7 мм; F4.5; e = 59° /1/100 000 /9 /18x18x51 /Бескорпусная, вынесенный объектив

WAT-903 (Watec - Япония) /2 • /350 /1/3" /D = 5 мм; F1.6; 9=67° /— /12 /40x65x35 /Бескорпусная, АРД

YC-05 (Computar - Япония) /2,5 /330 /1/3" /F 1,4; CS /1/50-1/20 000 /12 /55x40x100 /Цветное изображение

WV-CP210 (Panasonic -Япония) /1,5 /330 /1/3" /Fl,2; CS /1/50-1/20 000 /220 /67x65x118 /Цветное изображение

WV-BP310 (Panasonic -Япония) /0,02 /570 /1/3" /Fl,2; CS /1/50-1/10 000 /12 /— /—

Окончание табл. 1.4.8

Тип камеры (фирма - страна производитель) /Минимальная освещенность, лк /Горизонтальное разрешение телевизионных линий /Размер чувствительного элемента /Параметры объектива /Время срабатывания электронного затвора, с /Напряжение питания, В /Габариты, ММ (масса, г) /Примечание

PM200-L38 (Computar -Япония) /0,3 /380 /1/3" /D = 3,8 мм; F2.0; 9=63° /— /9 /32x32x18 /Бес корпусная

MD-38 (Computar -Япония) /0,3 /380 /1/3" /D = 3,8 мм; F2.0; 9=61° /— /9 /32x32x18 /Бескорпусная, вынесенный объектив

CEC—C38M (Computar -Япония) /0.6 /380 /1/3" /D = 3,8 мм; F2,0; 9=63° /— /9 /- /Бескорпусная

CA-H34CP (Kocom -Япония) /0,1 /380 /1/3" /D = 3,6 мм; F4,5; 9=65° /— /12 /54x30x23 /Бескорпусная, вынесенный объектив

VC-150 (Kocom-Япония) /0,2 /380 /1/3" /D = 3,6 мм; F4,5; 9=65° /— /12 /32x32x18 /Бес корпусная, вынесенный объектив

VPC-405G (Япония) /1 /380 /1/3" /D = 3,6 мм /— /— /— /Бескорпусная, АРД

JC-101 (Сотах) /0,1 /380 /1/3" /D = 3,6 мм; F2,0; /— /12 /— /Бескорпусная, вынесенный объектив

## 1.5. Перехват информации в линиях связи

### 1.5.1. Методы и средства несанкционированного получения информации в телефонных и проводных линиях связи

**Зоны подключения**

Рассмотрим потенциальные возможности перехвата речевой информации, передаваемой по телефонным линиям. Телефонную систему связи можно представить в виде нескольких условных зон (рис. 1.5.1). К зоне А относится сам телефонный аппарат (ТА) абонента. Сигнал с аппарата по телефонному проводу попадает в распределительную коробку (РК) (зона Б) и оттуда в магистральный кабель (зона В). После коммутации на автоматической телефонной станции (АТС) (зона Г) сигнал распространяется по многоканальным кабелям (зона Д) либо по радиоканалу (зона Е) до следующей АТС. В каждой зоне имеются свои особенности по перехвату информации, но принципы, на которых построена техника несанкционированного подключения, практически не отличаются.

Наиболее опасными зонами с точки зрения вероятности применения подслушивающих устройств считаются зоны А, Б и В.

Что собой представляет зона А общеизвестно, поэтому рассмотрим состав только линейных сооружений связи городских телефонных сетей (ГТС), куда входят абонентские линии, телефонная канализация со смотровыми устройствами и оконечное распределительное оборудование.

Телефонные линии служат для подключение аппаратов абонентов к городской АТС или телефонной подстанции и обычно состоят из трех участков (рис. 1.5.2): магистрального (от АТС до распределительного шкафа, РШ), распределительного (от РШ до распределительной коробки) и абонентского (от РК до телефонного аппарата).

Два последних участка (распределительный и абонентский) имеют сравнительно небольшую протяженность (80 % линий длиной до 3 км), но именно они являются наиболее уязвимыми с точки зрения возможного перехвата информации. Вследствие чего рассмотрим их структуру более подробно.

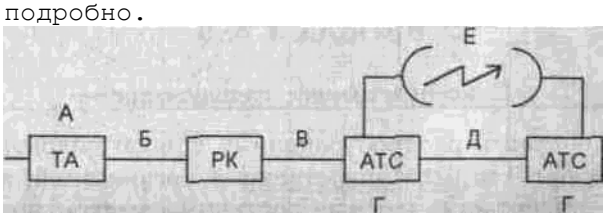



**Рис. 1.5.1. Основные зоны перехвата информация в каналах телефонной связи**


**Рис. 1.5.2. Основные элементы телефонной сети на участке «АТС-абонент»**

По системе построения телефонные линии разделяют на шкафные и бесшкафные, а по условиям прокладки — на подземные в специальной телефонной канализации, подземные в коллекторах и тоннелях, подземные бронированные, подводные, воздушные стечные, воздушные столбовые, настенные открытой прокладки, настенные скрытой прокладки и т. д.

На телефонных линиях, построенных по шкафной схеме, применяют следующее оконечное распределительное оборудование: боксы распределительных шкафов и распределительные коробки. На линиях, построенных по бесшкафной схеме, обычно используют кабельные ящики. Выпускаются распределительные шкафы типа РШ для размещения боксов общей емкостью 600 и 1200 пар, которые устанавливаются вне зданий, и распределительные шкафы типа РШП для размещения боксов общей емкостью 150, 300, 600 и 1200 пар, устанавливаемые внутри зданий. Стандартные распределительные телефонные коробки типа РК емкостью 10 пар устанавливаются внутри зданий на лестничных клетках, в коридорах, специальных слаботочных

совмещенных шкафах и нишах.
В сетях, построенных по бесшкафной схеме (что характерно для воздушных линий связи), используются кабельные ящики типа ЯКГ емкостью 10 и 20 пар, устанавливаемые непосредственно на опорах или чердаках одно- и двухэтажных зданий. Распределительные шкафы и кабельные ящики предназначены для соединения (кроссировки на боксах) магистральных и распределительных кабелей ГТС с целью наиболее экономичного построения и эффективного использования линейно-кабельной сети.
Знание структуры линии является определяющим при принятии решения об использовании того или иного типа аппаратуры перехвата.
ПЕРЕХВАТ ТЕЛЕФОННЫХ ПЕРЕГОВОРОВ В ЗОНАХ А, Б, В
**Непосредственное подключение**
Это самый простой и распространенный способ подслушивания телефонных разговоров. Для негосударственных организаций, занимающихся промышленным шпионажем, реально доступным местом подключения для перехвата информации являются зоны А, Б а В. Подключение бывает контактным и бесконтактным.
Шунт подслушивающего устройства в зонах А и Б может быть установлен в любом месте, где есть доступ к телефонным проводам или телефонному аппарату: в телефонной розетке или в любом другом месте телефонной линии на всем ее протяжении вплоть до распределительной коробки. В зоне В, при использовании магистрального кабеля, подключение подслушивающего устройства маловероятно. Это связано с тем, что для этого необходимо проникать в систему телефонной канализации, то есть в систему подземных сооружений, состоящую из одной или нескольких объединенных в блоки труб и смотровых устройств (колодцев), предназначенную для прокладки кабеля, его монтажа и осмотра. Таким образом, необходимо не только разобраться в хитросплетениях подземных коммуникаций, но и определить в многожильном кабеле нужную пару среди сотен и сотен ей подобных. При использовании воздушной линии задача значительно упрощается. Поэтому, когда вы принимаете решение, что использовать для телефонизации, например, вашего дачного поселка: подземный кабель, или дешевую «воздушку», то помните и о вопросах безопасности. Подземные кабели любителям да и многим спецслужбам пока не по зубам, однако, по мере роста профессионализма «шпионов» и улучшения качества защиты зон А и Б, зона В со временем тоже станет достаточно активно использоваться для проведения разведывательных операций.
В техническом плане самым простым способом незаконного подключения в зоне Б и В является контактное подключение (рис. 1.5.3).
Наиболее распространенный случай среди непрофессионалов — установка стационарного параллельного телефона. Возможно и временное подключение в любом месте абонентской проводки с помощью стандартного тестового телефона («монтерской» трубки) через обычный резистор номиналом 0,6... 1 кОм с помощью двух иголочек. Еще проще произвести подключение к РК или РШ. Эти, уж совсем примитивные, методы подробно рассматривать не будем, хотя они и включены в табл. 1.2.1. На практике такое подключение используется только полными профанами, поскольку очень велик риск быть пойманным.
Подключение к воздушной линии гораздо безопаснее и может производиться следующим образом: прокладывается пара очень тонких (с человеческий

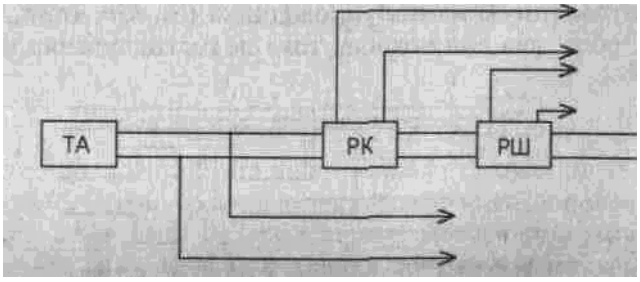



**Рис. 1.5.3. Контактное подключение к телефонной линии**

волос) покрытых лаком проводов от телефонной жилы или от монтажа лепестков распределительного ящика вниз по трещине деревянного столба к соседнему арендованному заранее помещению, где находится оператор, осуществляющий перехват.

Однако подключение такого типа имеет существенный недостаток: его довольно легко можно обнаружить из-за сильного падения напряжения, приводящего к заметному ухудшению слышимости в основном телефонном аппарате, что является следствием подсоединения дополнительной нагрузки. В связи с этим более эффективным является подключение с помощью согласующего устройства (рис. 1.5.4). Такой способ меньше снижает напряжение в телефонной линии, что значительно затрудняет обнаружение факта подключения к линии как самим абонентом, так и с помощью аппаратуры контроля.

Однако известен и способ контактного подключения к линиям связи с полной компенсацией изменения напряжения.

Подслушивающая аппаратура и компенсирующий источник напряжения при этом способе должны подключаться к линии последовательно, как это показано на рис. 1.5.5. Общим недостатком всех видов контактного подключения является необходимость нарушения целостности провода и влияние подключенного устройства на характеристики линии связи.

**Подключение бесконтактным методом**

В целях устранения последнего недостатка используется бесконтактный метод, при этом для съема информации обычно применяется индуктивный датчик, выполненный в виде трансформатора (рис. 1.5.6). При расположении такого устройства вблизи телефонной линии в нем будет наводиться напряжение, величина которого определяется мощностью передаваемого по линии сигнала и близостью обмоток датчика к проводам контролируемой линии. Однако в этом случае для нормальной работы устройства необходим усилитель звуковой частоты.

Иногда используются более сложные датчики, основанные на эффекте Холла (например, изделие **PRO 1219).** Датчик представляет собой тонкую прямоугольную пластину (площадью несколько квадратных мм) или пленку, изготовленную из полупроводника (Si, Ge, InSb, InAs) и имеет четыре электрода: два для подвода тока подмагничивания и два для съема


**Рис. 1.5.4. Подключение к телефонной линии через согласующее устройство**

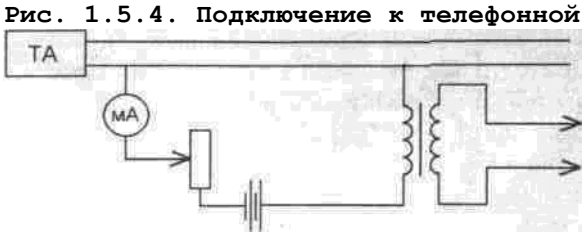


**Рис. 1.5.5. Подключение к телефонной линии с компенсацией падения напряжения**

информации. Чтобы избежать механических повреждений, пластинки монтируют (а пленку напыляют в вакууме) на прочной подложке из диэлектрика (слюда, керамика). Чтобы получить наибольший эффект, толщина пластины (пленки) делается возможно меньшей. Для повышения чувствительности датчик иногда монтируется в зазоре ферро- или ферромагнитного стержня.

Внешний вид некоторых индуктивных датчиков и варианты их подключения к кабелю показаны на рис. 1.5.7.

Качество принимаемого сигнала определяется не только подбором характеристик индукционного датчика, но также коэффициентом усиления и настройкой усилителя низкой частоты. При этом обязательно надо иметь регулируемую полосу пропускания. Это позволяет легко отфильтровать другие сигналы, наводки и помехи.

Подобные усилители в любом случае должны располагаться на выходе всех типов датчиков, что необходимо для оперативного прослушивания интересующего разговора. Должно быть предусмотрено и наличие гнезд для подключения магнитофона.

Впрочем, присутствие оператора совсем необязательно: в России имеется значительное количество датчиков для перехвата информации с телефонных линий в комбинации с диктофоном. Работа этой системы организована таким образом, что запись включается только при появлении сигнала в линии. Характеристики наиболее распространенных датчиков подобного типа приведены в табл. 1.5.1.

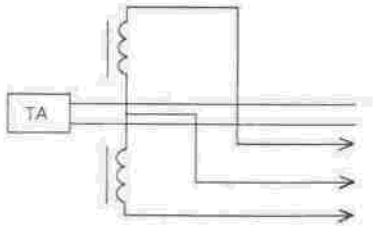



**Рис. 15.6. Способ подключения к телефонной. с помощью индуктивного датчика**

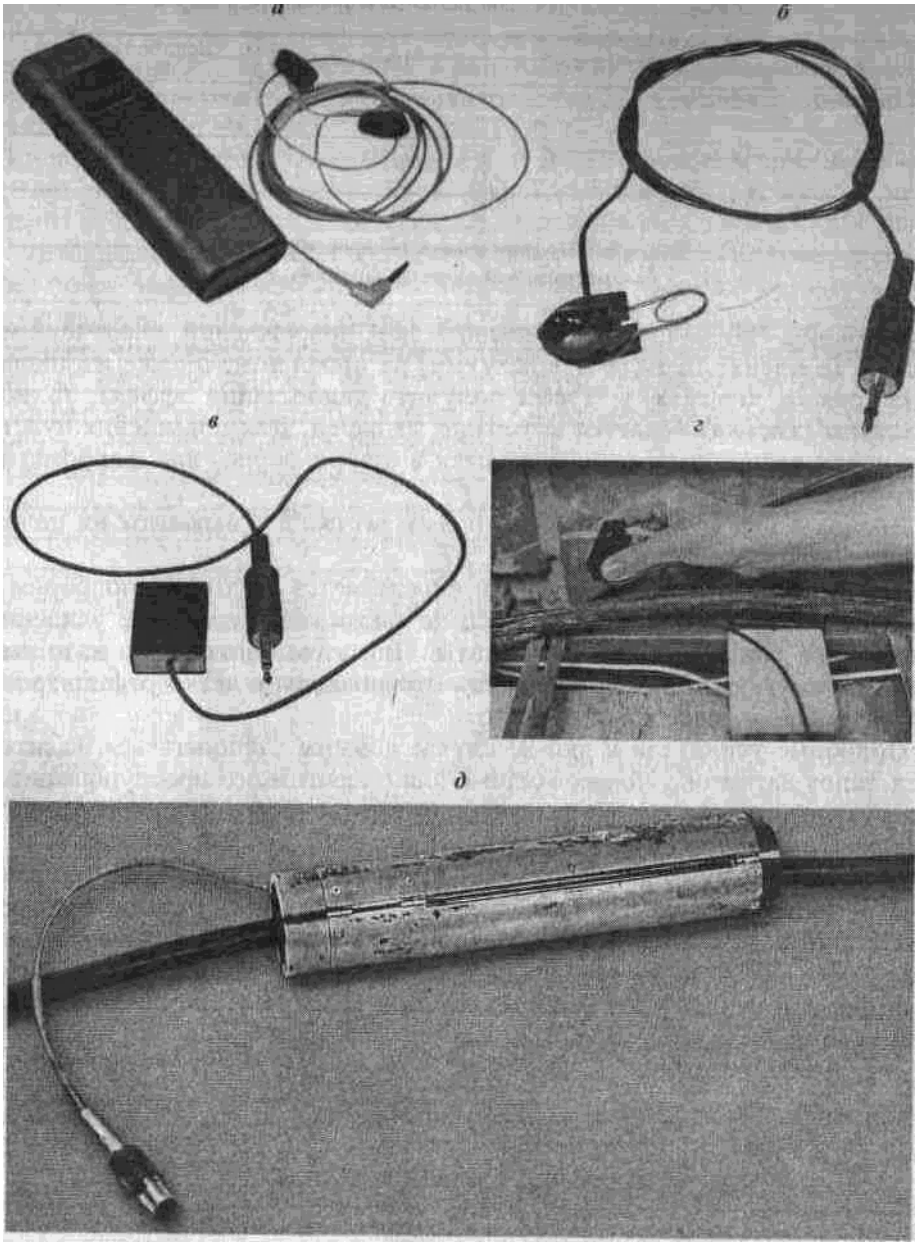


**Рис. 1.5.7. Индуктивные датчики:**
а — БД-1; б — «Клипса»; в — «Трамплин». Варианты подключения к телефонным линиям связи: г — в зоне Б; д — в зоне В

**Таблица 1.5.1. Датчики для записи телефонных разговоров**

Марка /Габариты, мм /Питание /Дополнительные функции
ЛСТ-АД /45х35х5 /Автономное /Автоматическое вкл./выкл.
ЛСТ-АД-11 /45х35х5 /3 В / 220 В /Автоматическое вкл./выкл.
ЛСТ-АД-2 /— /— /Автоматическое вкл./выкл.
ТТ-3 /35х25х20 /— /Автоматическое вкл./выкл.
БД-1 /— /Автономное /Индуктивный датчик
PRO 1213 /95х58х25 /Автономное, 9 В /Индуктивный зонд
PRO 1213 /95х58х25+50х22х10 /Автономное, 9 В /Эффект Холла
STG 4525 /125х75х25 /Автономное, 9 В /Индуктивный зонд
PRO 124 /80х60х20 /Автономное, 9 В /Регулируемая чувствительность

РК 135S /16х35 /Не требуется /Акустомат
UM 122 /100х50х18 /Автономное, 3 В /Контакт. Игла
УПМ-3 /50х20х20 /Автономное, 9 В /—
Стоимость подобных устройств колеблется от 20 до 250 $. В качестве записывающих устройств используются стандартные диктофоны типа SONY, Olimpus и др. В них применяются 90-минутные микрокассеты, что позволяет на минимальной скорости записывать до 3 часов телефонных переговоров. Ряд фирм выпускает магнитофоны с встроенными адаптерами для подключения к линии (табл. 1.5.2). Схемы параллельного и последовательного адаптеров приведены на рис. 1.5.8. В этом случае оператору достаточно просто произвести подключение к линии (в некоторых моделях только положить прибор на провод) и нажать кнопку «Запись». Главным недостатком указанных методов является необходимость иметь постоянный

**Таблица 1.5.2. Одноканальные магнитофоны для записи телефонных переговоров**

Марка /Габариты, мм /Питание /Время записи, ч /Дополнительные функции
ТТ-1 /— /Автономное /2 /Автомат, включение
PRO 153 /— /Автономное, 220 В /6 /2 скорости, акустомат
АД-2 /210х15х60 /Автономное, 220 В /2 /Акустомат
АД-3 /220х160х50 /Автономное, 220 В /12 /Акустомат, перемотка с памятью
СМВ-500 /— /Автономное /24 /Акустомат

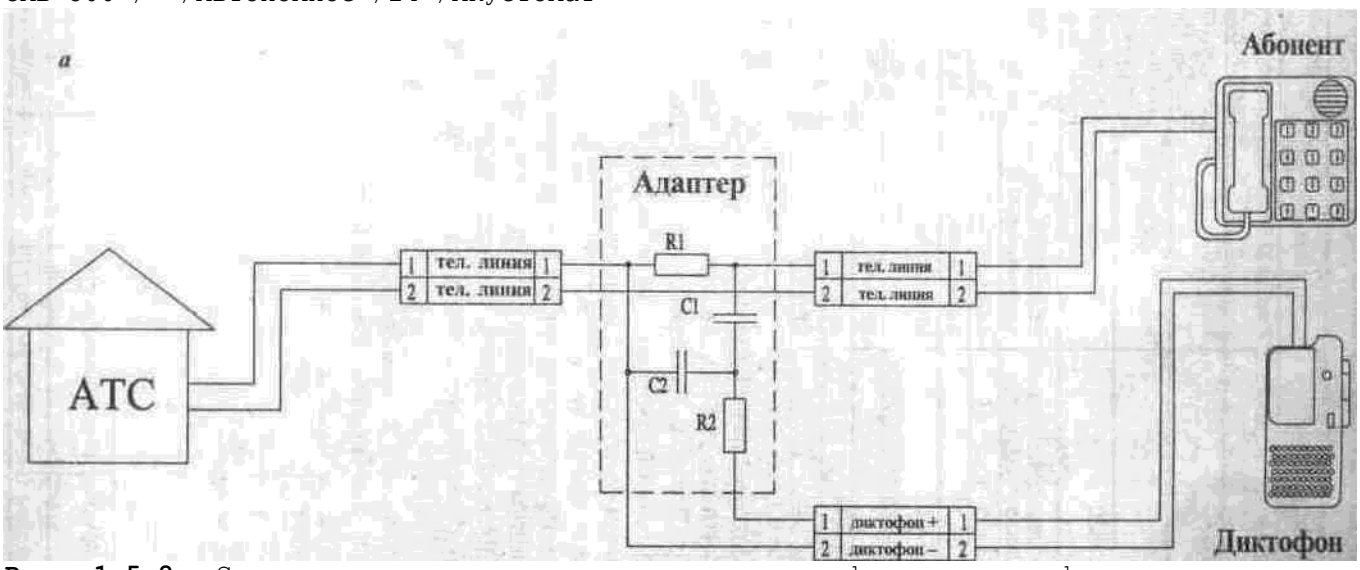



**Рис. 1.5.8.** Схемы адаптеров для подключения диктофонов к телефонным линиям связи:
а — последовательного типа, ток потребления не более 5 мА

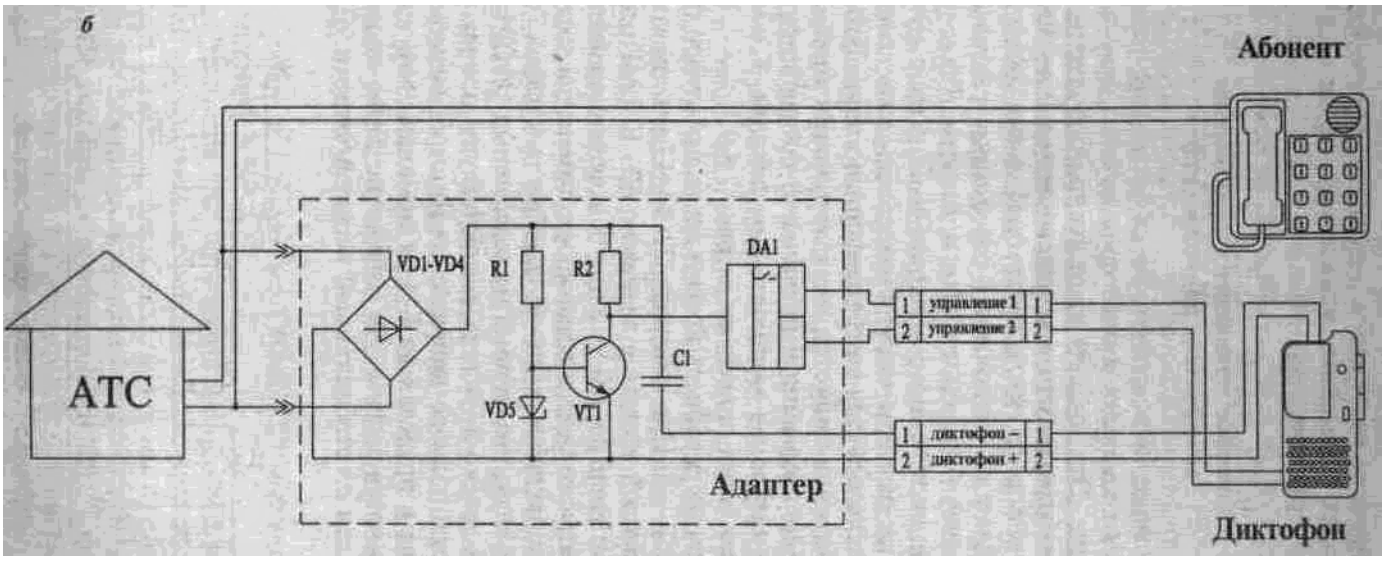



**Рис. 1.5.8. Окончание**

б — параллельного типа, ток потребления не более 1 мА

доступ в контролируемое помещение для смены кассет. Если это организовать невозможно, то применяют аппаратуру, передающую перехваченную информацию по радиоканалу.

**Основные принципы использования телефонных радиозакладок**

Телефонные закладки подключаются в любом месте телефонной линии и имеют практически неограниченный срок службы, так как питаются от контролируемой сети. Эти изделия чрезвычайно популярны в промышленном шпионаже благодаря простоте и дешевизне (от 9 до 400 $).

Большинство телефонных закладок автоматически включаются при снятии трубки и передают по радиоканалу телефонный разговор на пункт перехвата, где он может быть прослушан и записан. Такие устройства используют микрофон телефонного аппарата и не имеют своего источника питания, поэтому их размеры могут быть совсем небольшими. Обычно в качестве антенны используется сама телефонная линия. Это связано с тем, что специальная антенна является демаскирующим признаком, а кроме того от ее длины, согласования и правильной ориентации при установке напрямую зависит выходная мощность передатчика. Схема простейшей телефонной радиозакладки приведена на рис. 1.5.9.

Наибольшее распространение в России среди любителей получили дешевые изделия типа ЛСТ—5. При габаритах 22x14x13 мм эта закладка излучает сигнал на фиксированной частоте в диапазоне 60... 170 МГц, который может быть принят на расстояние до 400 м, а при подключении внешней антенны — даже до 1000 м. Предусмотрена и возможность изменения частоты в пределах ±10 МГц. Стоимость подобных изделий колеблется в районе 7...30 $.

Следует иметь в виду, что параметры телефонных сетей в России имеют большой разброс и далеко не всегда соответствуют принятым стандартам. Поэтому из-за нестабильного напряжения питания возможно изменение частоты передатчика в пределах до 1 % от номинала, что крайне осложняет процедуру вхождения в связь. Во избежание этого используются телефонные радиозакладки со стабилизацией несущей частоты. Для этого обыч-

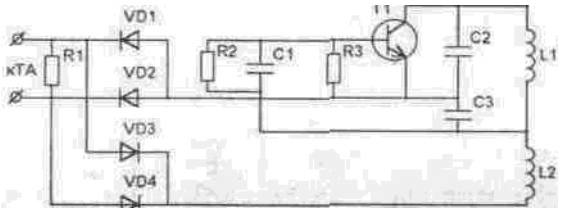



**Рис. 1.5.9. Радктелефонная закладка**

но применяются кварцевые резонаторы. Как правило, предлагаются изделия, работающие в диапазонах частот 100...150; 380...470 МГц. Конструкция прибора при этом существенно усложняется, стоимость вырастает до 40... 200 $, но потребительские качества значительно улучшаются. Не нужно судорожно «шарить в эфире» и гадать: ушла частота или выдерживается пауза в разговоре. В последние год-два телефонные радиозакладки с кварцевой стабилизацией частоты господствуют на рынке подобной спецтехники.

Выходная мощность передатчика в значительной степени определяется током потребления. Не рекомендуется увеличивать его более 2 мА, что определяется параметрами телефонной линии. Для большинства случаев развиваемой при этом мощности достаточно. Однако иногда возникают особые условия, например, возможна установка закладок внутри замкнутых металлических контуров (распределительных шкафов и т. д.), что приводит к снижению дальности перехвата в 2...7 раз. В этом случае возникает необходимость в использовании автономного питания. С целью упрощения подключений такого подслушивающего устройства и уменьшения его влияния на телефонную линию, а следовательно, и снижения вероятности обнаружения, часто применяется индуктивный датчик съема информации. Характерной особенностью подобных устройств является наличие собственного источника питания, что побуждает применять и системы автоматического включения передатчика в режим излучения только при снятии трубки телефонного аппарата. Качество перехватываемой информации практически всегда значительно хуже, чем у закладок с прямым подключением.

Для маскировки от обнаружения при визуальном контроле телефонные закладки, устанавливаемые в зоне А, выпускаются в виде конденсаторов, фильтров, реле и других стандартных элементов и узлов, входящих в состав обычного телефонного аппарата. Некоторые изделия, например, CRISTAL фирмы SIPE, сделаны в виде действующего микрофона телефонного аппарата и могут быть установлены в трубку абонента за несколько секунд. Есть образцы, выполненные в виде телефонной розетки (рис. 1.5.10).

Серьезной проблемой при работе вне зоны А является выявление нужной телефонной линии. Для этих целей используются специальные тестеры, например, типа UM 011.

UM 011 — прибор с габаритами 280x60x20 мм, весом 200 г и напряжением питания 3 В.

Для удобства использования он оборудован магнитной защелкой, которая позволяет установить корпус тестера на любом находящемся в месте работы металлическом предмете. В комплект входят иголки для прокалывания изоляции исследуемой проводки и специальные зажимы подключения провода тестера к этим иглам, а также светодиодный индикатор для определения состояния линии (красный — «занято», зеленый — «свободно»).

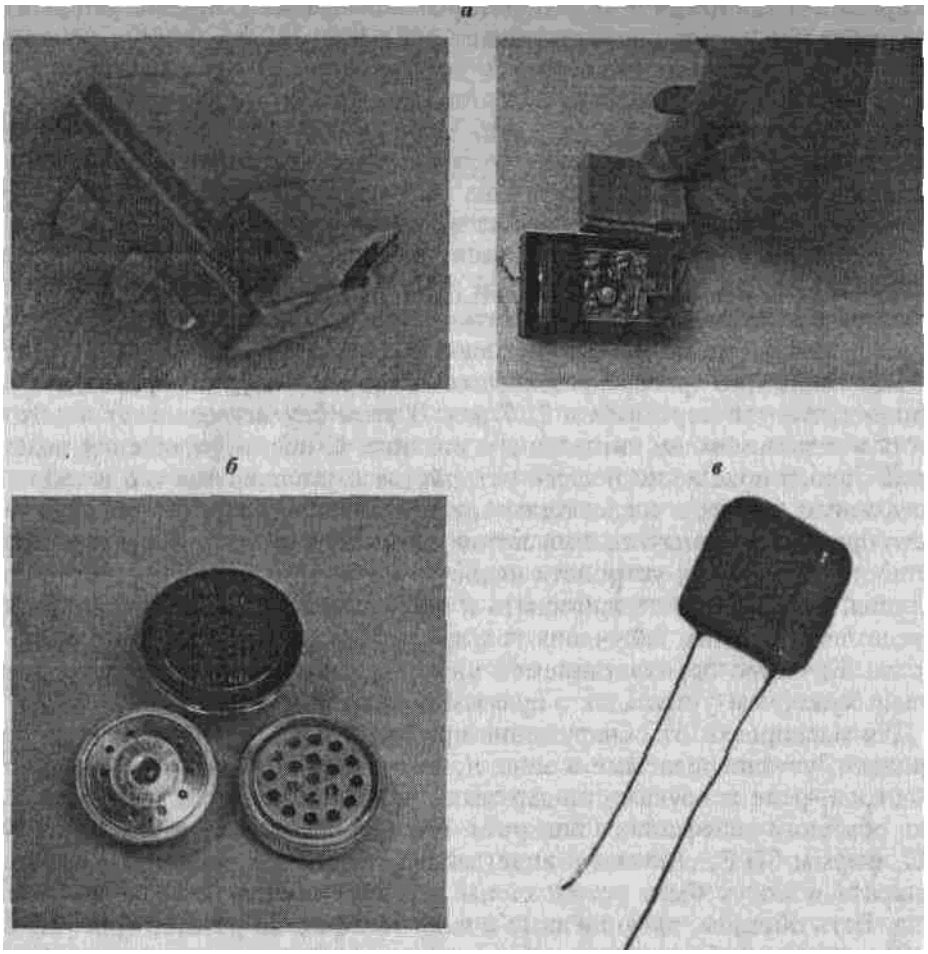



**Рис. 1.5.10. Радиозакладные устройства в виде элементов телефонной сети:**

а — в переходнике на евроразьем; б — в виде телефонного микрофона; в — в форме конденсатора

В случае, когда линия занята, прибор позволяет прослушивать разговор при помощи головных телефонов, подключаемых к гнезду «ТЛФ» тестера. А при необходимости позвонить предусмотрен номеронабиратель. Для этих же целей в комплект входит специальная перемычка для шунтирования линии в сторону контролируемого абонента, её применение исключает возможность выявления подключения за счет случайных звуковых сигналов на телефоне абонента при работе номеронабирателя тестера.

Профессионалы стараются установить телефонные радиозакладки за пределами офиса, что существенно снижает риск. Так, по сообщениям прессы, домашний телефон главы областной администрации Воронежской области прослушивался при помощи устройства, расположенного в распределительном шкафу в подъезде дома, где живет губернатор.

Во избежание возможности случайного перехвата передаваемых по радиоканалу телефонных переговоров какой-нибудь радиоприемной аппаратурой, а значит обнаружения факта подслушивания, в профессиональных закладках используются два основных приема: шифрация сигнала и применение нетрадиционных видов модуляции.

Использование криптографической защиты существенно увеличивает стоимость и ухудшает некоторые технические параметры телефонной радиозакладки (растут габариты, энергопотребление, снижается разборчивость речи и т. д.). В связи с этим, более перспективным

выглядит второй путь, то есть использование нетрадиционных для данной области видов модуляции. Например, амплитудная модуляция (АМ) с подавленной несущей или боковой полосой, использование поднесущих частот и т. д.

Перспективным направлением можно считать использование шумоподобных сигналов, которые очень сложно обнаружить без знания их параметров.

Одной из современных тенденций является использование системы с ретранслятором. При этом применяется простая радиозакладка с небольшим радиусом действия (обычно около 50 м). В безопасном месте устанавливается стационарный (или переносной) ретранслятор, переизлучающий сигнал закладки на значительные расстояния (до 10 км) часто на другой частоте и, возможно, в зашифрованном виде.

Для приема сигналов, излучаемых телефонными радиозакладками, используются устройства, аналогичные описанным в п. 1.3.1. Как правило, выделяют три основных типа:

>• бытовые приемники и магнитолы;

>• приемники различного назначения;

>• специальные приемники.

К первому типу, как указано выше, относятся обыкновенные бытовые приемники и магнитолы. Преимущество магнитол заключается в возможности записи информации, передаваемой по радиоканалу. К плюсам таких систем можно отнести их низкую стоимость и двойное назначение, как правило, окружающие их не замечают. Обычно они не вызывают никаких эмоций даже у сотрудников служб безопасности. К минусам относятся:

низкая чувствительность, что ограничивает дальность применения; использование общедоступного радиодиапазона (для отечественных приемников 62...74 МГц, для импортных 88... 108 МГц), что может привести к случайному перехвату вашего канала съема информации каким-нибудь любителем «пошарить в эфире».

Частично эти недостатки возможно устранить. Для этого осуществляют перестройку входных и гетеродинных контуров, что приводит к изменению диапазона рабочих частот до 110... 150 МГц у стандартных бытовых магнитол и пытаются несколько улучшить чувствительность. Другой путь связан с использованием конверторов, то есть устройств, осуществляющих перенос частоты принимаемого сигнала в рабочую область частот приемного устройства. В данном случае частотный диапазон может выбираться практически любой. При этом конверторы могут встраиваться непосредственно в приемное устройство (например, **ПРМ-450)**, либо выполняться в виде отдельных блоков (например, **СО-01**, фирмы «Вече») и при работе располагаться в непосредственной близости от бытового приемника. При использовании конверторов чувствительность приемного комплекса зависит как от технических характеристик самого преобразователя частоты, так и от характеристик собственно приемника и может достигать 0,9... 5 мкВ. Некоторое распространение получили конверторы с кварцевой стабилизацией частоты, которые не чувствительны к расположению окружающих предметов, в том числе, к касанию руками. В связи с этим отпала необходимость экранирования. К тому же, благодаря высокой шумовой и температурной стабильности кварцевого генератора, возможно зафиксировать настройку, а также значительно снизить шумы гетеродина.

Наиболее предпочтительно использование в качестве перестроенных магнитол изделия типа **Panasonic RQ-A160/A170**, **DAEWOO AHS-55W** и другой аналогичной продукции ведущих зарубежных фирм. Небольшие габариты (изделие свободно помещается в кармане куртки), относительно неплохой по чувствительности приемник и наличие возможности записи получаемой информации на стандартную кассету делают подобную аппаратуру достаточно удобной для работы с целым классом телефонных радиозакладок. В качестве

примера можно рассмотреть характеристики магнитолы AHS-55W.

**AHS-55W (DAEWOO)** — радиоприемное устройство, работающее в двух диапазонах частот: 88...108 МГц (FM) и 530...1605 кГц (АМ). Его габариты — 112x82,5x29 мм, вес — 250 г (без батареек). В диапазоне АМ используется встроенная магнитная антенна, а в диапазоне FM эту роль выполняет провод головных телефонов.

Цена подобных устройств во многом зависит от себестоимости базовой аппаратуры и колеблется в значительных пределах (15...400$).

Хочется отметить следующее. При записи сигнала на магнитофон возможно вскрытие набираемого на телефонном аппарате номера, а при наличии установленных у абонентов средств АОН — вскрытие и номера звонящего. Для этого необходимо иметь соответствующий программно-аппаратный комплекс обработки сигналов, например, декодер телефонных номеров **РК100** (габариты — 220x140x50 мм; вес — 1,5 кг; питание — 220 В). Впрочем, при некоторых навыках определить набираемый номер можно и на слух притом в реальном масштабе времени.

Ко второму типу можно отнести приемники различного назначения с более широким, чем у стандартной бытовой аппаратуры, частотным диапазоном. В последнее время значительное распространение получили многодиапазонные дешевые приемники (20... 150$ ) производства Германии, Китая, Южной Кореи. Рассмотрим характеристики подобных изделий на примере.

**Combicontrol 8000 Special** (фирмы **Pan** International) — частотный диапазон — 54...176 МГц; габариты— 206x96x53 мм; вес — 500 г; выходная мощность низкочастотного блока — 350 мВт.

Специалисты не любят подобную технику из-за крайне низкой чувствительности и значительных габаритов. «Юниоров» привлекает умеренность цены и простота в работе.

В конце 1991 года на отечественном рынке появились сканирующие приемники, в основном японского или немецкого производства. Сначала потенциальных покупателей отталкивала их достаточно высокая цена (400...2500 $). Однако несомненные достоинства подобной аппаратуры быстро сделали ее популярной. Имея небольшие размеры и высокую чувствительность, приемники могут использоваться с радиозакладками во всем возможном диапазоне частот и при любом виде модуляции. Наличие способности запоминать каналы и возможности сканирования по частоте позволяет работать одновременно с несколькими абонентами. Сканирование в заданной полосе позволяют легко работать с изделиями, несущая частота которых нестабильна. Кроме того, открываются и другие возможности.

Технические характеристики некоторых сканирующих приемников приведены в табл. 1.5.3. Более подробно об этом классе приборов будет сказано в разделе 2.4.

Настоящие профессионалы обычно используют третий тип приемников — специально разработанных. В качестве примера рассмотрим приемник **ЛСТ-П-3 (ЛСТ-П-5).** Чувствительность его — порядка 1 мкВ, диапазон рабочих частот — 110...160 МГц (или 400...450 МГц). Возможно подключение внешней антенны, например, автомобильной. Выход перехваченного сигнала — и на наушники, и на магнитофон.

Большинство специальных приемников настроено на одну частоту (в крайнем случае на 2...5 частот). Это позволяет добиться высокой чувствительности (0,5...3 мкВ при отношении сигнал/шум 20 дБ), сохраняя небольшие габариты и низкую стоимость. При создании таких приемников часто исполь-

**Таблица 1.5.3. Сканирующие радиоприемники, применяемые для работы с телефонными радиозакладками**

Модель /Диапазон, МГц /Вид модуляции /Чувствительность, мкВ (с/ш=12дБ) /Шаг перестройки, кГц /Количество каналов в памяти /Габариты, ММ /Вес, кг

IC-R1 /2...905 /AM, FM, WFM /0,4...3,2 /0,5; 1;5;8;9; 10; 12,5; 15; 20; 25 /100 /49x102,5x35 /0,3
PRO-42 /8...1300 /AM, FM, WFM /0,5 /5; 10; 12,5; 50; 100 /200 /65x159x40 /0,33
PRO-46 /29...956 /AM,FM /0,5...1,6 /12,5 /100 /66x151x37 /0,22
XR-100 (STABO) /0,53...1650 /AM, FM, WFM, LSB,USB /0,5...10 /0,05; 0,1; 1,5; 6,25; 9; 10; 12,5; 20; 25; 50; 100 /1000 /64,4x155x38,2 /0,32
MVT-7000 /8...1300 /AM, FM, WFM /0,5...1 /0,01; 0,1; 1;5;9; 10; 12,5; 20; 25; 100 / /159x64x40 /0,33
MVT-7100 /8...1300 /AM, FM, WFM /0,5...1 /0,01; 0,1; 1; 5; 9; 10; 12,5; 20; 25; 100 / /159x64x40 /0,33
AR-1500 /0,5...1300 /AM, FM, WFM /0,5...3 /5...995 (с шагом, кратным 0,05) /1000 /55x151x40 /0,33
AX-700E /50...904 /AM, FM, WFM /0,3...6 /10; 25;1000 /100 / /2
TR-980 /0,03... 1999,9 /AM, FM, WFM /0,5...2 /5; 10; 12,5; 25; 30 /125 /154x55x41 /0,270
Alan 1 /26...512 /AM,FM /0,2...5 / /50 /210x158x52 /1,2
Alan 1300 /8...1300 /AM, FM, WFM /0,5 /5...995 (с шагом, кратным 0,05) /100 /170x35x65 /0,3
AE39H /68...960 /AM,FM /1 / /200 /58x42x145 /0,25
PRO-50 /68...512 /AM,FM /1 / /20 /60x44x160 /0,26
AE44H /68...137 /AM,FM /1 / /50 /58x42x145 /0,25
BJ-200 MK /26...520 /AM.FM /0,5...1,5 /5;12,5 /16 /185x80x37 /0,47
DJ-XID /0,1...1299,9 /AM, FM, WFM /0,25...10 /5; 9; 10; 12,5; 20; 25; 30; 50; 100 /100 /53x110x37 /0,37

зуются специализированные микросхемы (например, К174ХА26) и микросборки (например, АК9401). Технические характеристики некоторых отечественных специальных приемников приведены в табл. 1.5.4.

Для записи телефонных переговоров часто используются специальные комплекты. Принцип их работы можно показать на примере изделия **«Телефонный секретарь».** В состав комплекта входит телефонная радиозакладка, устанавливаемая в разрыв линии, и приемник с магнитофоном, смонтированные в кейсе. При поднятии абонентом телефонной трубки происходит включение передатчика закладки, автоматический захват сигнала приемником и пуск (через 2 с) пишущего магнитофонного узла. Выключение магнитофона происходит мгновенно при пропадании сигнала. Удобство в работе подобного комплекта заключается в Том, что нет необходи-

Таблица 1.5.4. **Радиоприемные устройства отечественного производства, применяемые для приема излучений телефонных радиозакладок**

Модель /Диапазон, МГц /Чувствительность, мкВ (с/ш=2О дБ) /Тип антенны /Вид модуляции /Питание, В /Габариты, мм
ПРМ-М1 /100.,.115 /2...3 /телескопические /ЧМ /3 /135x60x18
ПРМ-1 /100...115 /1...3 /штырь /ЧМ /4,5 /-
UM 100 /105...108 /0,5...1/штырь /ЧМ /6 /-
UM101 /108...112 /0,5...1 /штырь /ЧМ /9 /-
ПРМ-М3 /108...115 /1 /штырь /ЧМ /6 /-
ЛСТ-П1 /110...150 /1 /штырь /ЧМ /9 /140x60x20
ПРМ-2 /115...130 /1...3 /штырь /ЧМ /4,5 /135x60x18
ПРМ-3 /130...150 /1...3 /штырь /ЧМ /4,5 /-
ПРМ-К /130...170 /1 /штырь /УЧМ /6 /150x60x20
UM100,2 /136...144 /0,5...1 /штырь /ЧМ /6 /-
UM042.1 /136...144 /0,5 /штырь /УЧМ,ЧМ /12 /140x95x30
РП-Ш270 /260...280 /3 /телескопические /ЧМ /9 /-

RA-04 /367...397 /2 /- /ЧМ /6 /-
RA-05 /375...385 /2 /штырь /ЧМ /10 /-
RA-07 /368...392 /2 /- /ЧМ /7 /115х55х22
ПРМ /391(417) /0,6...0,8 /штырь /УЧМ /6 /80х48х12
UM042.2 /412...430 /0,5 /штырь /УЧМ,ЧМ /12 /108х67х28

Таблица 1.5.5. **Телефонные радиозакладки**

Марка /Частота, МГц /Дальность передачи, м /Габариты, ММ /Вид модуляции
1 /2 /3 /4 /5

В обычном исполнении

ЛСТ-5 /60...170 /200... 1000 /25х13х10 /ЧМ
ЛСТ-7 /350...450 /300 /25х25х7 /ЧМ
GQ-205 /140...150 /150 /60х40х20 /УЧМ
PRO 136 /140...144 /до 2000 /40х24х12 /УЧМ
PRO 139 /135...180 /до 500 /36х12х10 /УЧМ
ПТ /88...108 130...150 /до 200 до 200 /31х9х7 31х9х7 /ЧМ ЧМ
Tl /90...118 /до 300 /14х13х8 /ЧМ
UM 003 /108...112 /до 500 /22х15х10 /ЧМ
UM 008 /136...145 /до 700 /22х15х10 /ЧМ
РТМ-12 /64...125 /50 /36х25х12 /ЧМ
РТП-017 /130 /100 /45х15х4 /ЧМ
РТП-018 /130 /— /70х25х4 /ЧМ
РТП-020 /380...470 /— /70х25х4 /ЧМ
РТШ-1 /262...278 /200 /45х22х10 /—
IPE005 /149...170 /250 /18х18х6 /УЧМ
EL330 /88...108 /100 /21х18х7 /ЧМ
SI-101 /88...108 /100 /14х14х24 /ЧМ
STG-4320 /135...145. /200 /— /УЧМ
STG-4310 /135...145 /200 /43х13х17 /УЧМ
STG-4311 /395...415 /200 /43х13х17 /УЧМ
АД-31 /398, 399 /360 /77х18х15 /УЧМ
АД-43 /398, 399 /300 /40х14х34 /ЧМ
РК140-SS /139 /1000 /45х15х14 /—
МТ602 /88...108 110...150 /200  200 /28х28х10 28х28х10 /ЧМ ЧМ

Продолжение табл. 1.5.5

Марка /Частота, МГц /Дальность передачи, м /Габариты, ММ /Вид модуляции
1 /2 /3 /4 /5

Кв.391 /391 /400 /78х18х5 /УЧМ
101-Р /88...108 /100 /24х14х14 /ЧМ
РТ-003 /88...108 /200 /19х12х10 /ЧМ

В закамуфлированном виде (под конденсаторы и другие радиотехнические элементы)

НВ-ПТ /130...150 /500 /3х16х4 /ЧМ
НВ-ПТ450 /400...500 /200...300 / /ЧМ
РК130 /138 /150 /«рисовое зерно» /ЧМ
РК130-S /138 /800 /15х6х11 /ЧМ
UM 008 /136...145 /До 700 /35х15х15 /ЧМ
TRM 1210...1270 /138 /50 /в габаритах камуфляжа /

Радиозакладки, установленные в капсулах телефонных трубок

РК(CRISAL) /— /150 /в габаритах камуфляжа /ЧМ
РК155 /— /300 /048х21 /ЧМ
РК110-S /— /250 /в габаритах камуфляжа /УЧМ

Комбинированные системы (телефон / микрофонные передатчики)

ЛСТ-4 /100...150 /100 /35х16х11 /ЧМ
ЛСТ-8 /350...450 /200 /25х25х5 /ЧМ
STG-4315 /115...150 /100 /26х22х15 /ЧМ
STG-4317 /395...415 /100 /66х27х14 /УЧМ
ПТРМ /88...108 130...150 /до 250 до 250 /29х19х12 29х19х12 /ЧМ ЧМ
РК125GHZ / /500 /25х20х10 /—
РК125-SS /139 /до 10000с ретранслятором /- /-



Окончание табл. 1.5.5

Марка /Частота, МГц /Дальность передачи, м /Габариты, Мм /Вид модуляции
1 /2 /3 /4 /5
Радиозакладки с индуктивным датчиком
Ш01т /100...210 /до 1000 /70х38х20 /ЧМ
Ш01ртм /100...210 /до 1000 /70х38х20 /ЧМ
Ш01т /100...210 /до 1000 /70х38х20 /ЧМ
Ш021т /100...210 /до 1000 /70х38х20 /ЧМ
STG-4320 /395...415 /250 /40х15х15 /УЧМ

мости в нахождении оператора на пункте контроля. Возможность питания комплекта от бортовой сети автомобиля 12 В позволяет осуществлять запись телефонных переговоров из машины, припаркованной недалеко от объекта контроля. Цена подобных изделий колеблется в пределах 100...8000 $.

Значительное место на рынке занимают комбинированные системы типа **ЛСТ-4**, которые позволяют осуществлять перехват как телефонных переговоров при поднятой трубке, так и разговоров в помещении при положенной трубке. Питание производится от телефонной линии. Однако дальность передачи информации небольшая, так как нежелательно увеличивать потребление тока от телефонной линии.

Характеристики некоторых телефонных радиозакладок приведены в табл. 1.5.5.

Использование телефонных радиозакладок возможно и для перехвата информации, передаваемой по факсимильной или телетайпной связи. Отличие состоит только в специальном устройстве обработки сигналов. Например, портативная аппаратура **TRM 3700**, подключаемая к выходу радиоприемного устройства, позволяет записывать информацию, передаваемую по телексу, на встроенный кассетный магнитофон или распечатывать на матричном принтере. Габариты системы — 475х395х180 мм, питание — 220 В, время непрерывной записи — 3 часа.

**Перехват побочных электромагнитных сигналов и наводок**

Любое электронное устройство при работе создает так называемые побочные электромагнитные излучения и наводки (ПЭМИН). Не является исключением и телефонный аппарат. Характерным примером являются широко распространенные аппараты с кнопочным номеронабирателем типа **ТА-Т, ТА-12, ТА-32** и т. д. При наборе номера и ведении переговоров, благодаря техническим особенностям блока питания, вся информация излучается на десятках частот в средневолновом, коротковолновом и ультракоротковолновом диапазонах. Это излучение может быть зафиксировано на расстоянии до 200 м. В случае применения подобного телефона радиозакладки совсем не нужны. Хочется отметить, что получившие широкое распространение телефонные аппараты с радиоудлинителем (Cordless Telephone) тоже значительно облегчают жизнь специалистам от промышленного шпионажа, так как дальность несанкционированного перехвата их довольно мощного сигнала достигает 400...800 м.

Конечно, приведенные примеры относятся к крайностям, но перехват

излучений может осуществляться с помощью малогабаритного индуктивного датчика, позволяющего улавливать побочные электромагнитные колебания практически любого телефонного аппарата на расстоянии до метра. При этом кроме речевых сигналов регистрируются также и сигналы набора номера. В качестве датчика используется катушка индуктивности. Она может быть плоской и устанавливаться там, где ее никто искать не будет, например, под основанием телефонного аппарата или под настольным письменным прибором, а также параллельно телефонному проводу внутри стен» под карнизами и плинтусами. Недостаток способа — появление наводок от посторонних источников.

Кроме самого аппарата, телефонные провода и кабели связи тоже создают вокруг себя магнитные и электрические поля, образующие каналы утечки информации за счет наводок на другие провода и элементы аппаратуры в ближней зоне.

Влияние одной линии на другую, когда они имеют определенный параллельный пробег, известно довольно давно. Отмечен даже исторический факт, имевший место еще в 1884 году, за 11 лет до изобретения радио А. С. Поповым. В Лондоне было обнаружено, что в телефонных аппаратах на улице Грей-Стоун-Род прослушиваются телеграфные передачи из какой-то другой сети связи. Проверка показала, что виноваты заложенные неглубоко под землей телеграфные провода, идущие на большом протяжении параллельно проводам телефонным. Величина наводимой энергии на параллельные линии зависит главным образом от длины параллельного пробега и от расстояния между проводами (рис. 1.5.11).

Отдельное место занимают системы, которые предназначены не для перехвата самих телефонных переговоров, а для акустического контроля помещений, где расположены телефонные аппараты или хотя бы проложены провода телефонных линий.

Поскольку именно эта тема особенно часто эксплуатируется авторами детективов, то рассмотрим этот вопрос достаточно подробно. Принципы и алгоритмы работы специальных устройств контроля помещения по телефонному каналу с дистанционным управлением проиллюстрируем на примере отечественных изделий **Elsy** и **UM 103.**

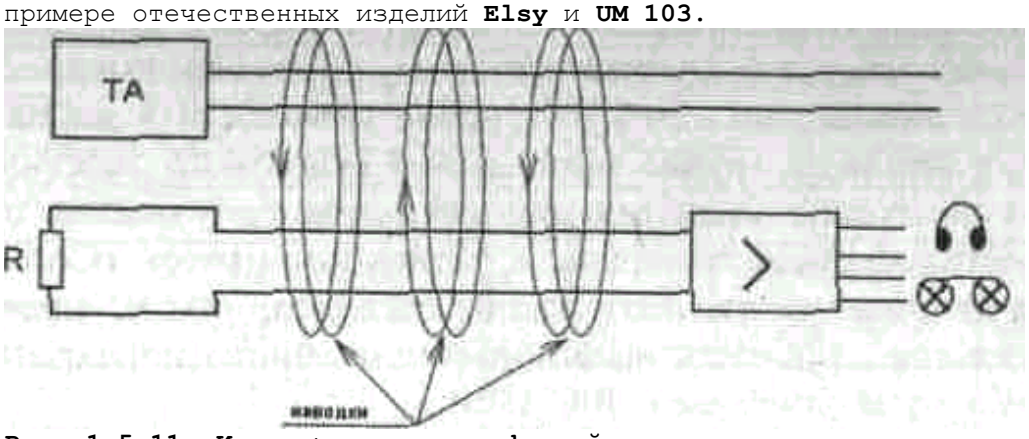



**Рис. 1.5.11. Использование телефонной сети для прослушивания разговоров в помещениях**

^Телефонное ухо» (Elsy) подключается параллельно к телефонной линии (розетке) в контролируемом помещении (рис. 1.5.12).

В принципе, наличия самого телефонного аппарата даже и не требуется, так как такая закладка может быть установлена в любом месте телефонной линии в пределах контролируемого помещения, например, в телефонной розетке. Поэтому те, кто, отсоединив свой аппарат от розетки, чувствуют себя в полной безопасности, могут жестоко ошибиться.

Для прослушивания помещения необходимо позвонить по номеру телефонного

аппарата (что можно сделать даже из другого города), на линии которого установлено устройство акустического контроля. После одного-двух стандартных гудков АТС «абонент не отвечает» происходит изменение их тональности, теперь необходимо произнести несколько слов (или подать любой звуковой сигнал). Акустическая закладка активируется и начнет передавать информацию из помещения по телефонной линии, притом с достаточно хорошим качеством.

Положительным моментом является то, что система питается от телефонной сети. Недостаток этих комплексов очевиден: полная зависимость от поведения абонента телефонного номера, к которому осуществлено подключение. Сдерживает их широкое применение и довольно высокая стоимость.

К зарубежным аналогам можно отнести устройство **Telemonitor.** Единственным его отличием от вышеописанного является возможность подключения до четырех датчиков к системе на одну линию для контроля различных помещений. Кроме того, на сам телефонный аппарат три первоначальных звонка вообще не проходят.

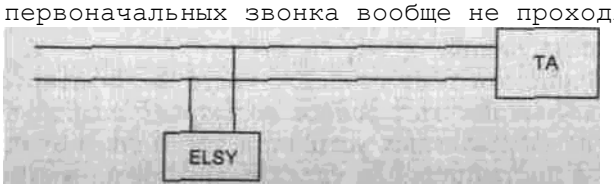



**Рис. 1.5.12. Принцип применения закладного устройства типа Elsy**

Изделие UM 103 подключается аналогично Elsy, но имеет выносной микрофон (рис. 1.5.13), что упрощает маскировку самого прибора в помещении. Алгоритм функционирования изделия следующий: при поступлении сигнала вызов на аппарат контролируемого абонента UM 103 «проглатывает» первые два звонка, после чего телефонный аппарат совершенно нормально работает. Для включения устройства необходимо позвонить контролируемому абоненту, подождать гудка станции, положить трубку, отсчитать нужное количество секунд (индивидуальный временной код доступа) и набрать его телефон снова. В трубке будет слышен сигнал «занято». Необходимо подождать 45 с и UM 103 включится на прослушивание. Стоимость комплекта — порядка 5000 $.

Однако высокая цена фирменной аппаратуры не должна настраивать вас на мажорный лад: как это не покажется парадоксальным, но изготовить упрощенную версию прибора этого типа может даже радиолюбитель средней руки. Для иллюстрации приведем принципиальную схему устройства дистанционного прослушивания помещений с использованием телефонной линии (рис. 1.5.14), разработанную одним из радиолюбителей и рекламируемую в популярном журнале как охранная система. Устройство состоит из двух частей; приемно-передающего блока, устанавливаемого на контролируемом объекте, и мини-передатчика звуковых сигналов (бипера), включающего этот' блок.

Принцип действия аппаратуры прост. Приемно-передающий блок в любом удобном месте подсоединяют к телефонной линии и подают на него напряжение питания от сети 220 В или от автономного источника +12 В. Теперь достаточно только позвонить по «зараженному» номеру с любого телефона и, услышав гудки «абонент не отвечает», прислонить к микрофону своей трубки включенный бипер. Дальше происходит следующее. В работу включается трансформатор Т1 (конденсаторы С1 и С2 в его первичной обмотке препятствуют шунтированию линии) и передает сигнал с обмотки II на трехкаскадный усилитель (транзисторы VT1—VT3). Усиленный сигнал следует на селективное реле К1. Последнее включает реле времени К2, определяющее промежуток времени, в течение которого устройство будет работать на передачу. Этот интервал устанавливается с помощью потенциометра R 10. После включения реле К2 блокирует себя контактами

К2.1, контактами К2.2 включает передатчик, а контактами К2.3 имитирует снятие трубки, чтобы подключить на АТС к линии звонивший телефон.

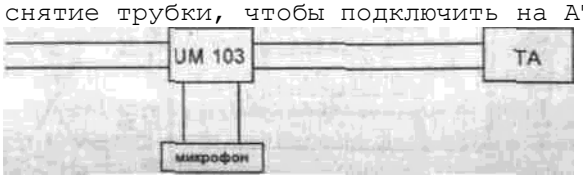



**Рис. 1.5.13. Принцип применения закладного устройства UM 103**

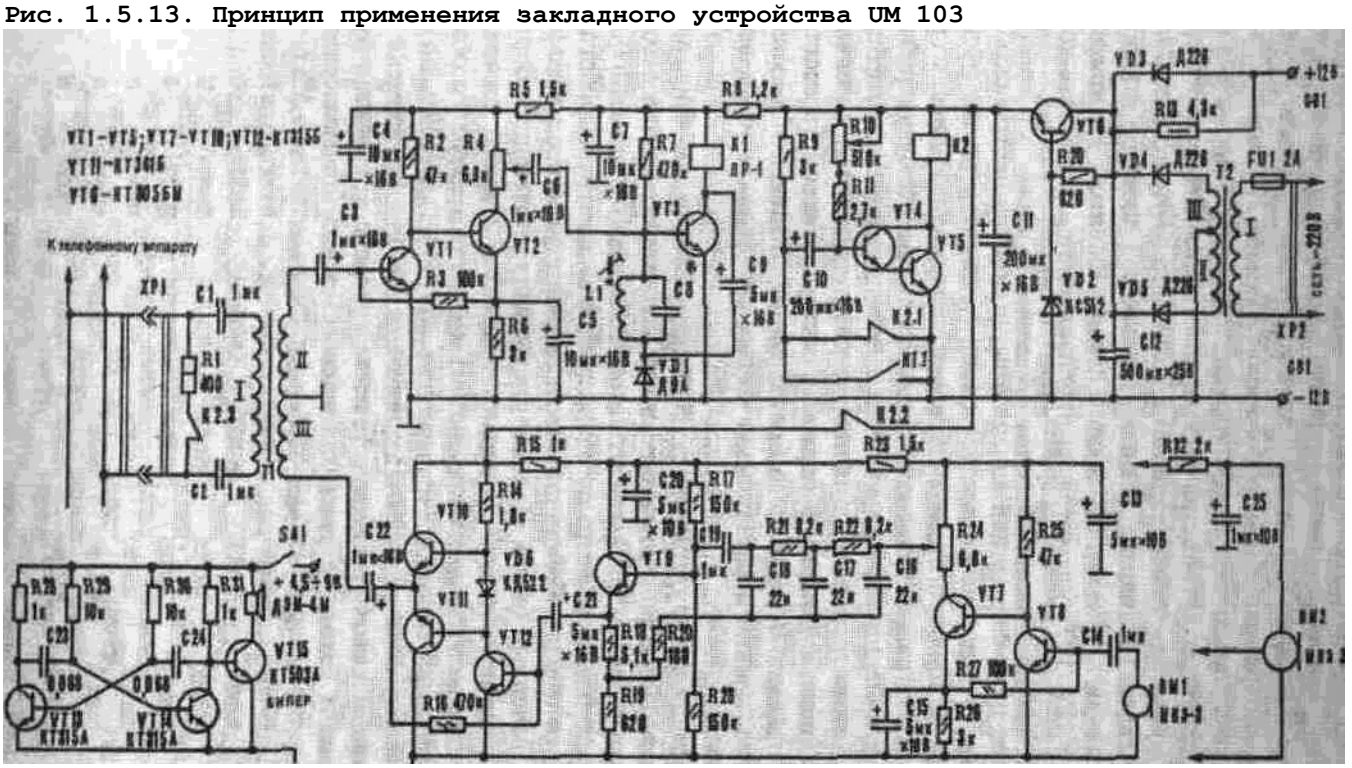


Рис. 1.5.14. Принципиальная схема телефонной закладки типа «телефонное ухо»

Передатчик состоит из микрофона ВМ1 с двухкаскадным усилителем (транзисторы VT8 и VT9), устройства коррекции, представляющего собой заградительный фильтр, и двухкаскадного оконечного усилителя (транзисторы VT10—VT12). Нагрузкой выходного каскада, собранного по двухтактной схеме, служит обмотка III трансформатора Т1, через которую сигнал с микрофона поступает в телефонную линию.

Детали, используемые в устройстве, — самые типовые, широко распространенные. Трансформаторы 77 и 72 идентичны промышленному Б-22. Реле легко изготовить из трех герконов, работающих на размыкание. Налаживание системы заключается в настройке передатчика на частоту 1000 Гц и доводке приемного устройства, которая сводится к регулированию селективного реле с помощью конденсатора С10. Что касается бипера, то он — не что иное, как типичный мультивибратор, нагруженный на динамик ДЭМ-4М. Как видите, богата наша земля талантами, поэтому не стоит расслабляться и сбрасывать со счетов системы подслушивания, увидев в каталоге цену со многими нулями.

Кроме того, возможно использование телефонной линии и для постоянной передачи информации с микрофона, установленного в помещении. Чтобы «не засветить» микрофон, используется несущая частота в диапазоне от десятков до сотен килогерц с целью не препятствовать нормальной работе телефонной связи. Одним из вариантов реализации подобной системы является комплект **ST-01**, состоящий из приемника и датчика. Датчик типа **Р10** устанавливается в телефонной розетке. Для передачи используется

частота 100 ±10 кГц. Модуляция — частотная. Ток потребления — не более 2,5 мА.

Приемник сигналов **ST-01** имеет:

- систему автоматической регулировки уровня сигналов на выходе;
- ручную регулировку уровня сигнала на головных телефонах;
- регулятор тембра голоса;
- систему контроля состояния элементов питания;
- систему контроля наличия несущей частоты в телефонной линии;
- систему контроля наличия информационного сигнала.

Для регистрации информации к приемнику подключаются наушники или диктофон. Частотный диапазон приемника на линейном выходе по уровню 6 дБ — 300...3300 Гц. Дальность передачи не превышает 200 м, поскольку ВЧ-сигналы сильно затухают в телефонной линии.

Практика показывает, что в реальных условиях дальность действия подобных систем с приемлемой разборчивостью речи может быть еще меньше и существенно зависит от целого ряда факторов: качества телефонной линии; способа прокладки телефонных проводов; наличия в данной местности радиотрансляционной сети; наличия вычислительной и иной техники и т. д. Главным недостатком этого типа аппаратуры, помимо высокой стоимости, является большое количество времени, затрачиваемого на ее установку и необходимость проникновения в контролируемое помещение.

Для любого специалиста, работающего в области промышленного шпионажа с применением технических средств разведки, представляют наибольший интерес так называемые беззаходовые системы, то есть комплексы средств, позволяющие получать информацию из интересующих помещений без необходимости физического проникновения в них, которое зачастую просто невозможно. Телефонный аппарат предоставляет в этом плане определенные возможности. Неслучайно даже некоторые высокопоставленные чиновники опасаются вести компрометирующие разговоры в собственных кабинетах, кивая при этом на телефонный аппарат. Этот, конечно же, сильно преувеличенный страх нельзя считать совершенно беспочвенным, поскольку есть три потенциально возможных варианта прослушивания помещения с помощью телефона:

- телефонный аппарат содержит систему передачи информации, то есть в его конструкцию целенаправленно внесены соответствующие изменения или просто установлена специальная аппаратура типа описанной выше;
- используются определенные недостатки конструкции стандартного телефонного аппарата;
- производится такое внешнее воздействие на телефонный аппарат, при котором он превращается в канал утечки акустического сигнала из помещения.

Так как первый случай достаточно подробно уже рассмотрен, познакомимся с возможностями, которые дает применение второго варианта.

Причиной возникновения канала утечки информации в этом случае являются электроакустические преобразования, возникающие в некоторых узлах телефонного аппарата, например в катушке звонка. При разговоре акустические волны воздействуют на маятник звонка, который в свою очередь соединен с якорем электромагнитной катушки. Под этим воздействием якорь совершает микроколебания, а это вызывает колебание якорных пластин в электромагнитном поле катушки, что приводит к появлению в цепи звонка наведенных токов, модулированных речью. Как известно, цепь звонка при положенной трубке непосредственно включена в линию.

По данным специальных исследований, амплитуда сигнала, наводимого в линии, для некоторых типов телефонных аппаратов может достигать нескольких милливольт. Для приема этих наводок может быть использован

обыкновенный усилитель низкой частоты (УНЧ) с диапазоном 300...3500 Гц, который просто подключается к абонентской линии (рис. 1.5.15). В качестве такого приемника возможно, например, использование многофункционального

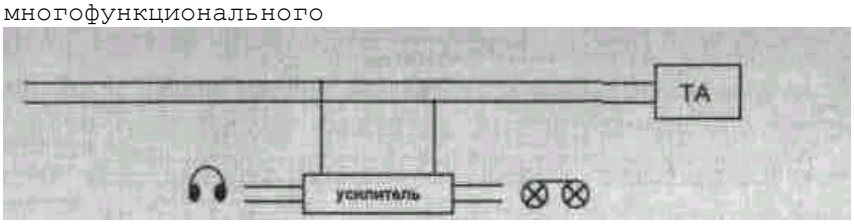



**Рис. 1.5.15. Прием информационных сигналов, возникающих в результате акусто-электрического преобразования**

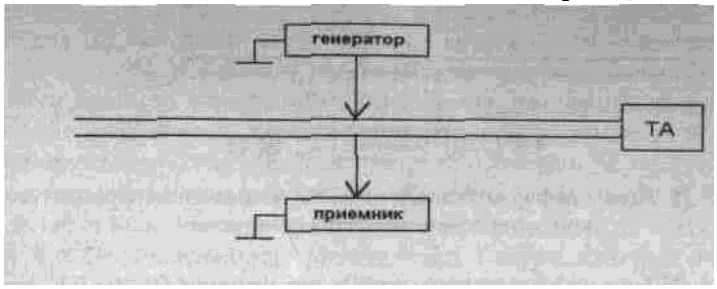
УНЧ типа **UM 053** с коэффициентом усиления порядка 7000. Батарея напряжением в 9 В обеспечивает непрерывную работу прибора, имеющего габариты всего 150x65x30 мм, в течение 50 часов.

Недостатком этого, на первый взгляд, очень перспективного, способа является то, что сигнал в большинстве случаев слишком слабый, и дальность действия подобной системы даже с хорошей аппаратурой не превышает нескольких десятков метров (зона Б). Данное обстоятельство существенно снижает практическую ценность второго варианта в реальных условиях.

Третий вариант получения информации связан с явлением так называемого ВЧ-навязывания. Он заключается в том, что относительно общего корпуса (в качестве которого лучше использовать землю, трубы отопления и т. д.) на один провод подается ВЧ-колебание с частотой от 150 кГц и выше. Через элементы схемы телефонного аппарата, даже если трубка не снята, а значит отсоединена от сети, зондирующее ВЧ-излучение все-таки поступает на телефонный микрофон, где и модулируется речью. Прием информации производится относительно общего корпуса через второй провод линии. Амплитудный детектор позволяет выделить низкочастотную огибающую для дальнейшего усиления и записи. Очевидно, что для повышения качества перехватываемой информации желательно производить подключение как можно ближе к телефонному аппарату (опять зона Б), что существенно снижает эффективность применения системы. Работа системы показана на рис. 1.5.16. Более подробно это материал изложен в п. 1.3.5.

ПЕРЕХВАТ ТЕЛЕФОННЫХ ПЕРЕГОВОРОВ В ЗОНЕ Г

В этом случае наиболее безопасно организовать стационарное прослушивание телефонных разговоров, что достаточно просто сделать на телефонной станции (коммутаторе). В народе бытует мнение, что на телефонных станциях сутками напролет сидят представители спецслужб и прослушивают все переговоры. На самом деле это совсем не так. Во-первых, на станциях сидеть вовсе не обязательно — достаточно подключиться к единой системе АТС. Более того, прослушивать все




телефонные разговоры

**Рис. 1.5.16. Реализация принципа высокочастотного навязывания в телефонных линиях связи**

нет необходимости. Контроль идет выборочно, по заданным номерам, так как анализ перехваченных телефонных разговоров и ведение

соответствующих досье требует длительной, кропотливой работы. В связи с этим круг абонентов ограничен. Так, ЦРУ в многомиллионной Мексике контролировало в 60-е годы всего 40 телефонных номеров. При этом, наряду с дипломатами стран Варшавского Договора, прослушивались телефоны прокоммунистических организаций, мафиозных лидеров, а также политических деятелей (вплоть до экс-президентов) и членов их семей. Кроме того, эпизодически контролировались переговоры деятелей науки и культуры с мировым именем.

Аналогичная ситуация складывалась и в бывшем СССР, где, по некоторым данным, прослушивались телефоны иностранных представительств, лиц, подозреваемых в совершении преступлений, различного рода диссидентов, а также руководителей различного ранга. Кроме того, иногда записывались разговоры родственников интересующих лиц и людей из их ближайшего окружения. Так, прослушивались переговоры парикмахера Р. М. Горбачевой, тренера Б. Н. Ельцина по теннису и т. д.

Прослушивание телефонных переговоров — достаточно дорогостоящее мероприятие. В связи с этим оно, как правило, не проводится на постоянной основе. Например, телефоны экс-лидера Афганистана Бабрака Кармаля в Москве прослушивались всего две-три недели. Так как ничего интересного не обнаружили, то контроль прекратился.

В качестве примера организации стационарного пункта можно привести операцию по прослушиванию телефонных разговоров, проводимую американской резидентурой совместно с полицейским управлением Монтевидео. Необходимые подключения к телефонным линиям на АТС производились инженерами телефонной компании по просьбе полицейского управления. Шестидесятижильный кабель протянули от центрального телефонного узла в деловой части города к полицейскому управлению, где на верхнем этаже размещался пункт прослушивания. Там находились исполнительные механизмы и аппаратура записи. Обслуживали пост два техника, которые передали записи в аналитический пункт.

В СССР до середины 80-х годов телефонные переговоры контролировались только спецслужбами и правоохранительными органами. Как утверждал бывший глава КГБ Вадим Бакатин, до августовского путча 1991 года 12-й отдел КГБ СССР прослушивал в Москве примерно 300 абонентов, в основном иностранных граждан и преступников. Контроль служебных переговоров велся и на особо режимных объектах, но здесь следили не за конкретным человеком, а за утечкой секретной информации. В этом случае использовались специальные системы контроля, работающие по ключевым словам и позволяющие прерывать (блокировать) или телефонный разговор в целом, или отдельные фразы. При этом легко устанавливались номера абонентов — нарушителей режима. Однако аппаратура для подобного контроля стоила очень дорого — порядка 200 тысяч рублей (в ценах 80-х годов) и применялась только на крупных объектах оборонной промышленности ив правительственных учреждениях.

Если верить уже упомянутому «Совместному решению по эксплуатационно-техническим требованиям к средствам и сетям электросвязи для обеспечения оперативно-розыскных мероприятий», то в России в состав сетей электросвязи вводятся аппаратные и программные средства, позволяющие проводить контроль из удаленного пункта управления. Кроме того, должна быть предусмотрена возможность по командам из пункта управления изменять на определенный период состав услуг, предоставляемых отдельным абонентам, а также осуществлять конспиративное подключение выделенных службе безопасности каналов и линий к любым абонентским линиям (каналам), в том числе уже находящимся в состоянии соединения.

Однако пока крайне редки случаи коммерческого прослушивания на городских АТС, так как это невозможно без наличия там «своего» человека

из обслуживающего персонала.
Сейчас для обеспечения телефонной связью крупных организаций, гостиниц, предприятий и т. д. в них создается своя телефонная сеть, обслуживаемая самостоятельной учрежденческой АТС. Эта сеть предоставляет всем своим абонентам внутреннюю телефонную связь, а некоторой группе абонентов — право связи с абонентами ГТС, а через ГТС с междугородной телефонной станцией.
Как известно, значительное внимание службы безопасности серьезных предприятий уделяют контролю телефонных переговоров своих сотрудников. Идеальным местом подключения специального многоканального магнитофона как раз и является местная АТС. Там в миниатюре возможно повторить действия спецслужб.
На отечественном рынке многоканальные магнитофоны еще представлены слабо. Пока многоканальность создается использованием большого числа стандартных или специальных одноканальных магнитофонов, характеристики которых приведены в табл. 1.5.6. За рубежом имеется значительное число образцов подобной техники. Как правило, это специально

**Таблица 1.5.6. Специальные многоканальные стационарные устройства записи телефонных переговоров**

Марка /Количество каналов /Габариты, ММ /Вес, кг /Время записи, ч /Дополнительные функции

РК115-S /10 /500x360x150 /9,8 / /Автоматическое вкл. Подключение принтера, привязка ко времени

РК100-SS /1 10 50 100 /205x1666x290 1100x550x380 110x890x660 2200x1890x600 /2,9 60 220 430 /4 10x4 50x4 100x4 /Автоматическое вкл. Подключение принтера, метки даты и времени, сигнализация о сбоях в работе и переполнении кассеты

CU-1 /10 / / /Переменная /Регистрация времени, числа, номера абонента, подсчет числа звонков

AD-25 /8 /480x350x190 /16 / /Метка времени, дистанционное управление

ТМ /9; 20; 31; 42 / / /до 1000 /Регистрация числа, времени, автоконтроль

разработанное устройство предназначено для стационарной записи телефонных переговоров и рассчитано на значительное число каналов (от 10 до 100).
Часто устройства имеют модульную структуру, которая позволяет наращивать их возможности до требуемого уровня.
Различные компании предлагают значительное количество дополнительных сервисных функций у такого рода аппаратуры. В качестве примера рассмотрим компьютеризированное устройство **DNR-600**, которое позволяет проводить анализ 2500 телефонных линий на предмет активности. При этом регистрируются время, дата, набираемый номер, продолжительность разговора и т. д. В памяти может храниться информация о 400 звонках на каждую линию.
Существует более простая аппаратура прослушивания и записи телефонных переговоров на 16 телефонных линий типа **WORLDSAFE.** Особенностью ее является то, что 24-часовая запись производится на обыкновенную видеокассету стандарта VHS. Внешнее управление аппаратуры возможно осуществлять с персонального компьютера через интерфейс RS 232. Записи распознаются по содержанию информации или по маркерам, установленным оператором. Два канала могут прослушиваться одновременно или раздельно через стереонаушники. К дополнительной возможности относится наличие индикатора занятости линии. Надежность записи обеспечивается механическим ключом, имеющим 4 уровня защиты.
Существует система, записывающая разговоры на медленно движущуюся стальную проволоку, которая по надежности превосходит обычную магнитную

ленту. Как правило, это две бобины, с одной из которых на другую перематывается несколько сот метров проволоки. Система фиксирует как время переговоров, так и номера абонентов, с которыми шел разговор. Эта же система может распечатать содержание разговоров. Кроме того, в некоторых случаях предусматривается возможность срабатывания только по кодовым словам.

Широкое распространение офисных АТС привело к необходимости решения задач контроля их сигналов. Офисная АТС по сути своей является коммутатором внешних городских линий и внутриофисных линий связи. Сложность в осуществлении контроля внешних линий связи часто возникает из-за того, что при входящих и особенно исходящих вызовах трудно определить линию, по которой идет информация. Это связано с динамическим распределением вызовов по линиям. Иногда эти проблемы решаются с помощью программ фиксированного распределения входящих звонков. Абонентские внутриофисные линии близки к внешним городским линиям по ряду основных параметров, а различие заключается в номинале напряжения (ГТС имеет 60 В, офисная сеть —24 В) и способах его подачи на абонентские аппараты.

При включении в такие линии связи аппаратуры подслушивания с питанием от телефонной сети или входным сопротивлением менее 100 кОм съем информации становиться невозможен. В связи с этим датчики подключаемых устройств должны иметь высокое сопротивление как по постоянному, так и по переменному току.

Для удобства работы операторов таких многоканальных систем прослушивания создано целое семейство вспомогательных устройств. Например, прибор типа **РК10-04-005** позволяет осуществлять перезапись 120-минутной магнитофонной кассеты менее чем за 2 мин.

Существует мнение, что передача информации по факсу или телексу повышает безопасность информации. На самом деле это не так. В настоящее время разработаны десятки устройств перехвата факсимильных сообщений. Технически это не сложнее восстановления обычного телефонного разговора, да и способы подключения практически те же. В качестве примера рассмотрим устройство **FAX-MANager.** Будучи подключенным к телефонной сети, оно различает телефонные и факсовые сообщения и принимает их независимо друг от друга, а также автоматически копирует и хранит в памяти все послания, получаемые или отправляемые по факсу. При этом система может зафиксировать практически любое количество страниц и воспринимает информацию, передаваемую со скоростью от 300 до 9000 бит/с.

Перехваченные послания распечатываются четко и с высоким разрешением. Прибор в принципе может быть установлен в любом месте на линии (в зонах А, Б, В), но обычно подобная аппаратура устанавливается именно в зоне Г. При этом система работает в совершенно автономном режиме.

Более современная модель FAX-MANager-2 позволяет осуществлять запись перехваченных сообщений на магнитофон. Подобные устройства предлагаются как в переносном, так и в стационарном вариантах. Разработаны и многоканальные системы прослушивания факсимильной связи тип **CD-3.** Эта система постоянно прослушивает 10 телефонных линий и делает печатные копии входящих и исходящих сообщений. Имеются индикаторы, показывающие, когда линия свободна, а когда используется для телефонной или факсимильной связи. Может комплектоваться системой дистанционного управления наружным магнитофоном, прерывателем передачи информации и устройствами записи на компьютер.

Разработана и широко используется аппаратура и для прослушивания телексов. Например, система CD-3 одновременно контролирует до 10 телексных линий. Возможна распечатка перехваченных сообщений либо визуальный просмотр и распечатка только тех, которые представляют

определенный интерес.

ПЕРЕХВАТ ТЕЛЕФОННЫХ ПЕРЕГОВОРОВ В ЗОНЕ Д

Перехват информации с многоканальных линий связи как кабельных, так и волоконно-оптических, и выделение телефонных переговоров абонентов, за которыми ведется наблюдение, представляют собой очень сложную задачу, которая пока не под силу отечественным специалистам от промышленного шпионажа (по крайней мере, факты подобных подключений еще не известны, хотя интерес к подобной аппаратуре большой и стоит она относительно недорого).

Доступ к коаксиальным кабелям затруднен, поскольку они заглублены и, кроме того, во многих случаях заключены в герметическую оболочку, находящуюся под давлением. При этом нарушение целостности оболочки приводит к падению давления и срабатыванию тревожной сигнализации. В случае, если кабель не находится под давлением, необходимо наличие следующего оборудования для осуществления перехвата:

**>•** гальванический отвод.....25 $;

**>•** демультиплексор, соответствующий полосе модулирующих частот.....5000 $;

**>•** смеситель.....50 $;

**>•** устройство декодирования сигналов вызова.... 1000 $;

**>•** магнитофон..... 100 $.

Таким образом, полная стоимость подобного комплекта — чуть более 6000 $.

Плюс к этому необходимо иметь одного-двух специалистов по монтажу линий связи. По некоторым данным, первые опыты подобного рода проводились офицерами разведки Австро-Венгрии на Итальянском фронте еще в августе 1915 года.

Более сложной и универсальной аппаратурой, которая может применяться для съема информации с любых кабельных линий связи, пользуются современные спецслужбы. Рассмотрим принцип ее действия на примере американской системы **«Крот»**.

С помощью специального индуктивного датчика, охватывающего кабель, снимается вся передаваемая по нему информация. Для проникновения к кабелю используются колодцы. Датчик устанавливается на кабель в колодце и для маскировки проталкивается в трубу, что исключает его обнаружение при периодическом осмотре колодца монтером. Высокочастотный сигнал, идущий по кабелю, записывается на магнитный диск специального магнитофона. После заполнения диск заменяется новым. Запись с диска передается спецслужбе и обрабатывается приборами демодуляции и прослушивания. В целях упрощения задачи поиска устройства «Крот», что необходимо для замены диска, оно снабжено сигнальной радиостанцией. Агент, проезжая или проходя в районе установки прибора-шпиона, запрашивает его с помощью своего портативного радиопередатчика, все ли в норме. Если аппаратуру не трогали, то она передает соответствующий сигнал. В этом случае при благоприятных условиях агент заменяет диск в магнитофоне и работа устройства продолжается. Аппарат может записывать информацию, передаваемую одновременно по 60 телефонным каналам. Продолжительность непрерывной записи на магнитофон составляет 115 часов. Такие устройства находили в Москве в начале 90-х годов.

Более десяти аналогичных «Кротов» по просьбе сирийской стороны было снято нашими специалистами в Дамаске. Там все подслушивающие устройства были закамуфлированы под местные предметы и заминированы на «неизвлекаемость». Часть из них при попытке изъятия все-таки взорвалась.

Перехват информации с подводных линий связи — крайне сложное и дорогостоящее мероприятие. Тем не менее подобная аппаратура типа **«Камбала»** применяется разведкой США. «Камбала» — достаточно сложное

устройство с ядерным (плутониевым) источником электропитания, рассчитанным на десятки лет работы, предназначено для съема информации с подводных бронированных кабелей связи.
Устройство «Камбала» выполнено в виде стального цилиндра длиной более 5 м, диаметром 1200 мм. В герметически закрытой трубе смонтировано несколько тонн электронного оборудования для приема, усиления и демодуляции снятых с кабеля сигналов. Запись перехватываемых разговоров осуществляется 60 автоматически работающими магнитофонами, которые включаются при появлении сигналов. Каждый магнитофон рассчитан на 150 часов записи. Таким образом, общий объем записи может составить около 9 тысяч часов. К моменту, когда пленки израсходованы, подводный пловец находит устройство подслушивания по гидроакустическому маяку, установленному на контейнере, снимает с кабеля индукционный датчик-захват, предварительный антенный усилитель и доставляет устройство на специально оборудованную подводную лодку. Это огромное устройство в воде имеет почти нулевую плавучесть. В лодке осуществляется замена магнитофонов, после чего устройство вновь устанавливается на линию связи. В контейнере смонтирована система приема, усиления и демодуляции ВЧ-сигналов, проходящих по кабелю. Специальный чувствительный индуктивный датчик способен снимать информацию с подводного кабеля, защищенного не только изоляцией, но и двойной броней из стальной ленты и стальной проволоки, плотно обвивающих кабель. Сигналы с датчика предварительно усиливаются антенным усилителем, а затем направляются для демодуляции, выделения отдельных разговоров и их записи на магнитофоны.
Следует учесть, что для практического применения такой системы необходима еще специальная подводная лодка, оборудованная устройством для поиска подводных кабелей в морских глубинах. Понятно, что найти в море кабель даже в том случае, когда известна трасса его прохождения, — задача не простая. Для поиска кабеля нужны специальные электронные приборы с датчиками, находящимися вне лодки, приспособленными для работы на глубине.
«Камбала» опробована в деле для контроля наиболее важных каналов связи среди множества советских подводных кабельных коммуникаций. По признанию американцев, это были, пожалуй, самые опасные операции, когда подвергались риску жизни всех людей на борту подлодки, — экипажа и спецгруппы АНБ. Каждая операция утверждалась лично президентом. Атомная подводная лодка выходила в море, в заданном квадрате устанавливались звукозаписывающие устройства (их называли «коконы»), затем она уходила из этого квадрата и выжидала несколько недель. Потом возвращалась в тот же квадрат, чтобы снять пленки с установленного на кабеле записывающего устройства.
Директор ЦРУ признавал: «Иногда подлодка возвращалась с довольно богатым урожаем сведений о советских вооруженных силах. Как и при других подобных операциях, все строилось на ошибках другой стороны. Русские считали, что подводные кабели прослушивать невозможно, и поэтому использовался сравнительно несложный шифровальный код, а иногда обходились и без него».
Операция в Охотском море успешно осуществлялась до 1981 года. Но однажды на фотоснимке с американского спутника было отмечено большое скопление советских судов как паз в том участке Охотского моря, где к кабелю было прикреплено подслушивающее устройство. Один из советских кораблей был оборудован подводной спасательной техникой. Ранее было зафиксировано участие этого судна в спасательных операциях в различных районах мирового океана. Позднее, когда американская подводная лодка прибыла для замены пленок, она обнаружила, что устройство исчезло. Была создана комиссия по расследованию, которая установила, что поскольку

русские точно вышли к месту, то они знали, что делают, значит у КГБ есть агент.
Провал операции подхлестнул активную деятельность американской разведки. Предлагалось скрытно провести из Гренландии глубоководный кабель и с его помощью подслушивающие устройства подсоединить к советским подводным коммуникационным линиям в северных прибрежных водах. В этом случае информация сразу же попадала бы в Агентство национальной безопасности (АНБ) в реальном масштабе времени. Расстояние между Гренландией и советским побережьем составляет около 1200 миль. При всей заманчивости от этого плана отказались: кабель пришлось бы укладывать на дно океана при цене около 1 млн $ за милю. По другому проекту, стоимостью уже несколько миллиардов долларов, предлагалось, используя такую же технологию, прослушивать все коммуникационные кабели мира.
Таким образом, в настоящее время имеется целое семейство спецсредств перехвата информации с кабельных линий связи: для симметричных ВЧ-кабелей — устройства с индуктивными датчиками, для коаксиальных и НЧ-кабелей — с системами непосредственного подключения и отвода малой части энергии для целей перехвата. Для кабелей, внутри которых поддерживается повышенное давление воздуха, применяются устройства, исключающие его снижение, в результате чего предотвращается срабатывание специальной сигнализации. Некоторые приборы снабжаются радиостанциями для прямой передачи перехваченных разговоров в центр обработки. Однако из-за их колоссальной стоимости данные системы применяются только спецслужбами очень богатых стран.
Значительный интерес представляет возможность перехвата информации с волоконно-оптических линий связи (ВОЛС). По некоторым данным, в настоящее время до 10 % всех линий передачи информации, а к 2000 году — почти все вновь вводимые линии будут волоконно-оптическими. Уже разработан и опробован оптический телефон и проводится работа по созданию принципиально новых АТС.
Считается, что использование оптических волокон в качестве физической среды для передачи большого объема информации по сравнению с существующими электрическими кабелями в части, касающейся защиты информации, имеет следующие преимущества:
- высокая помехозащищенность (устойчивость к воздействию окружающей среды, электромагнитным и оптическим помехам);
- гальваническая развязка по питанию различных элементов сети;
- отсутствие излучений и наводок на соседние информационные линии и устройства;
- сложность несанкционированного подключения.

Сутью несанкционированного доступа к оптическому волокну является Создание (или использование природной) неоднородности, на которой происходит рассеяние части сигнала. Далее с помощью оптического приемника осуществляется перехват информации.
Примером природной неоднородности является место соединения ВОЛС. Причинами возникновения излучения в разъемных соединениях волоконных световодов являются: радиальная несогласованность стыкуемых волокон; угловая несогласованность осей световодов; наличие зазора между торцами световода; наличие взаимной непараллельности поверхностей торцов волокон; разница в диаметрах сердечников стыкуемых волокон. Все эти причины приводят к излучению световых сигналов в окружающее пространство.
По мнению специалистов фирмы Dell Communication Research (США), возможен перехват информации с ВОЛС. Для этого требуется длительный контроль линий с помощью приборов, широко применяемых для неразрушающего контроля качества волоконно-оптического кабеля (ВОК) при

его производстве и испытаниях.
В одном из способов перехвата используется свойства ВОК излучать небольшое количество энергии в месте его изгиба. ВОК зажимается между двумя пластинами, одна из которых имеет рифленую поверхность, предназначенную для деформации волокна. На другой пластине размещается фотодетектор и устройство регистрации информации.
При другом варианте схеме подключения в качестве элемента съема светового сигнала используется стеклянная трубка, заполненная жидкостью с высоким показателем преломления и с изогнутым концом, жестко фиксированная на оптическом кабеле, с которого предварительно снята экранная оболочка. На отогнутом конце трубки устанавливается объектив, фокусирующий световой поток на фотодиод, а затем на усилитель звуковых сигналов подается уже электрический сигнал с фотодиода.
В самом простом варианте подключения (так называемое контактное подключение) идут еще дальше: просто удаляют защитные слои кабеля, светоотражающую оболочку и изгибают его на необходимый угол. Даже при таком грубом подключении к ВОК обнаружить утечку информации за счет ослабления мощности бывает очень трудно. Так как при существующих приемных устройствах аппаратуре несанкционированного доступа достаточно отобрать всего 0,001 % передаваемой мощности, чтобы уверенно подслушать переговоры, а дополнительные потери при изгибе кабеля составляют всего 0,01...! дБ в зависимости от его угла.
ПЕРЕХВАТ ТЕЛЕФОННЫХ РАЗГОВОРОВ В ЗОНЕ Е
В последнее время большой популярностью среди бизнесменов пользуются радиотелефоны и радиостанции различных типов. Среди них, наряду с импортными, появляются и отечественные образцы. Как это ни странно, но существует расхожее мнение, что при разговоре по обычному телефону возможность его прослушивания существенно выше, чем при разговоре по радиотелефону. Увы, мы вынуждены развеять эти иллюзии, но сначала необходимо описать принцип работы самих радиотелефонов.
Радиотелефон — это в сущности комплекс из двух радиостанций, одна из которых является базовой, устанавливается стационарно и подключается к телефонной сети, вторая — подвижная. От обычной, радиостанции они отличаются тем, что пользователь выходит непосредственно в ГТС.
Следовательно, осуществлять прослушивание радиотелефонных разговоров, с одной стороны, в принципе можно теми же способами, что и обычных телефонных. Однако с точки зрения съема информации радиотелефоны, в том числе сотовые системы, и радиостанции объединяет то, что при работе они сами используют радиоволны. Следовательно, достаточно приобрести качественный приемник с соответствующим диапазоном частот, хорошую антенну, устройство звукозаписи и без всякого риска «подключиться» к разговору. При этом дальность радиоперехвата будет не меньше дальности работы радиотелефона, а при использовании хорошей аппаратуры — в несколько раз больше. Так, если радиус действия базовой станции сотовой связи составляет от 5 до 15 км, то перехват при определенных условиях возможно осуществлять на расстоянии до 50 км. Дальность будет зависеть от многих факторов, в первую очередь от высоты расположения антенны, ее направленных свойств и от чувствительности приемника.
Мобильные сети связи для «узкого круга» существуют в России уже много лет, примерно с 60-х годов. До сих пор в некоторых городах России действует система **«Алтай»**. В Москве, например, у нее около 6 тысяч пользователей. Различие между системой «Алтай» и современными системами в том, что первая не является сотовой.
Сотовой называется система связи, состоящая из множества ячеек, которые, связываясь между собой, образуют широкую сеть. Система «Алтай» работает с единственной ячейкой, к которой подключены все абоненты. Именно потому, что сотовые сети имеют возможность наращиваться и

соединяться между собой, они и стали так популярны.
Система «Алтай» работает в диапазоне 150 и 300 МГц, сотовые системы используют диапазон 450, 800 и 900 МГц (стандарты NMT, AMPS, GSM). Кроме того, некоторое распространение в России получили телефонные интерфейсы, предназначенные для удобной и надежной связи между радиокоммуникационным оборудованием и стандартными телефонными системами. Подобные средства, например **TW5800**, позволяют отдаленным радиостанциям устанавливать связь с телефонными абонентами и наоборот. Часто абонент и не предполагает, что его переговоры транслируются на десятки и сотни километров и становятся легкой добычей радиолюбителей. Известно немало случаев, когда осуществлялся перехват информации в этих каналах с коммерческими целями. Так, у немецкой фирмы «Шмидтунд Фольке», которая конкурировала с другими компаниями в разработке месторождений на дне моря, был похищен ее самый ценный секрет: точное географическое положение обследуемого района. Агенты прослушивали радиосвязь плавучей конечной станции фирмы с ее вычислительным центром на суше и затем обрабатывали полученную информацию. Результаты своих трудов они продавали конкурирующей фирме, которая благодаря этому сэкономила значительную сумму, так как разведка месторождений полезных ископаемых на больших глубинах всегда связана с весьма крупными затратами.
Наиболее скандальный случай — прослушивание переговоров по сотовому телефону короля Испании Хуана Карлоса испанскими же спецслужбами (кстати, в Испании в спецподразделениях по контролю телефонной связи всего шесть человек). Заодно прослушивали премьер-министра, министра иностранных дел и высокопоставленных гостей страны, и без счета — обычных бизнесменов, журналистов и т. д.
Кроме того, необходимо помнить, что по излучаемым сигналам можно установить местоположение подвижных объектов, оборудованных радиотелефоном.
Одним из наиболее универсальных разведывательных приемников является **Miniport** фирмы «Роде и Шварц» с диапазоном рабочих частот 20... 1000 МГц. С его помощью можно без труда осуществлять перехват всех радиостанций и радиотелефонов. Данный приемник имеет небольшие габариты (188x71x212 мм), универсальное питание (от аккумуляторной батареи и от сети 220 В) и может успешно применяться как в стационарных, так и в полевых условиях. Управление приемником осуществляется цифровым способом через встроенный процессор. Визуальное считывание значения частоты производится с цифрового дисплея с шагом 1 кГц. Запоминающее устройство микропроцессора может хранить в памяти до 30 фиксированных частот и осуществлять сканирование в заданном диапазоне с переменным шагом. Возможности приемника могут быть существенно расширены за счет совмещения с малогабаритным анализатором спектра, специально для него разработанного, — типа **EPZ100**. Для удобства применения комплекса аппаратуры в полевых условиях поставляются укладочные кейсы, где отдельно размещается аккумулятор, приемник с анализатором спектра и набор антенн.
Известно, что определение местоположения (пеленгация) работающих на излучение радиостанций производится с помощью вращающихся в горизонтальной плоскости специальных антенн направленного действия. Для определения точного местоположения источника сигнала необходимо иметь несколько, по крайней мере два пеленгатора, чтобы сделать «засечку» в месте пересечения двух пеленгов одного источника с разных мест. В последнее время появились более совершенные пеленгаторы доплеровского типа, у которых нет механически вращающихся антенн, а есть одна антенная мачта, на которой установлено более десяти идентичных дипольных антенн. За счет специальной обработки сигнала производится

мгновенная пеленгация излучателя. При совмещении подобной антенны с описанным выше приемником возможно за 0,1 с обнаружить радиосигнал, измерить его параметры и определить пеленг. С учетом необходимости передачи данных на другой пост пеленгации, с целью однозначного определения местоположения источника излучения, требуется около 1—2 с для точного определения места. Таким образом, не успев сказать несколько слов по радиотелефону, абонент, точно указывает местоположение своего автомобиля.

Современные передающие устройства могут использовать перестройку частоты в ходе сеанса связи по случайному закону, осуществлять передачу с использованием специальных видов модуляции, что затрудняет перехват информации.

Фирма Telefunken System technik проектирует, разрабатывает и производит радиопеленгаторы серии **Telegon** в частотном диапазоне 10 кГц...1 ГГц. Данные пеленгаторы отличаются высокой чувствительностью и могут перехватывать кратковременные и слабые сигналы при перегруженности диапазона частот. При этом предусмотрена возможность перехвата сигналов и с перестройкой частоты.

Иногда, для упрощения контроля за перемещением объекта, используются специальные радиомаяки, которые скрытно устанавливаются в автомобилях, а в некоторых случаях вшиваются в одежду, монтируются в портфеле, калькуляторе и других вещах объекта наблюдения. Подобное устройство было установлено в печатной машинке одного бывшего сотрудника ЦРУ, благодаря чему отслеживались все его перемещения с квартиры на квартиру. Известны случаи установки подобных устройств в полостях каблуков обуви, возвращенной после ремонта.

Обычно подобные маяки имеют режим прослушивания разговоров, ведущихся объектом наблюдения.

Значительное распространение сотовой связи и особенности ее организации привели к необходимости создания специальной, гораздо более сложной аппаратуры для осуществления ее контроля. Дело в том, что телефоны этого типа не привязаны к фиксированным частотам, а могут работать на любой свободной частоте в пределах своего поддиапазона, что значительно затрудняет перехват. Более подробно данные вопросы будут изложены в подразделе 1.5.2.

Рассмотрим работу систем перехвата сообщений из каналов сотовой связи на примере **STG 4610 и STG 4615**. Основой подобных устройств являются специальные радиоприемные устройства с декодером сигналов сотовой связи. Используя технику цифровой обработки сигналов для расшифровки неслышных служебных сообщений, идущих между сотовым телефоном и сотовой станцией, декодер позволяет оператору настраиваться на частоту телефонов и автоматически прослушивать разговор через свой аппарат без перерывов в приеме. Подобные системы обычно оснащаются индикаторными устройствами отображения частоты и уровня принимаемого сигнала, встроенными магнитофонами, специальными антеннами, комбинированными источниками питания и другими необходимыми устройствами. На российском рынке предлагается весьма эффективная аппаратура контроля сотовых сетей стандартов **NMT-450 и AMPS** по цене до 20 тысяч $.

Проблема перехвата существенно усложняется, если в сотовой сети предусмотрена криптографическая защита речевой информации. Однако даже и в этом случае полной гарантии (как это делают телефонные компании) дать нельзя, поскольку существуют специальные комплексы радиоперехвата с возможностью анализа зашифрованных сигналов, например **Sigint/Comint Spectra** фирмы Hollandes Signaal. Подобная аппаратура чрезвычайно дорога (более 100 тысяч $) и может использоваться только организациями, обладающими очень большими средствами. Данных о наличии подобных систем в России в частном владении нет, но надо помнить, что потратив

определенную сумму, вас вполне могут слушать «заинтересованные лица».
Большую популярность получила пейджерная связь, которая осуществляется следующим образом. Абонент городской АТС набирает один из номеров пейджерной компании и передает сообщение диспетчеру, который вводит его в компьютер. Дальнейшая передача сообщения осуществляется автоматически по радиоканалу. Существуют и полностью автоматические системы. Через 2 года после появления данного вида связи в России были разработаны и предлагаются покупателям программно-аппаратные системы перехвата. В состав подобной системы входят: специально доработанный сканер **(AR-3000A, IC-7100** и т. д.); устройство преобразования; ПЭВМ и специальное программное обеспечение. Система позволяет осуществлять прием и декодирование текстовых и цифровых сообщений, передаваемых в каналах радиопейджинговой связи, и сохранять все принятые сообщения (с датой и временем передачи) на жестком диске ПЭВМ. При этом может производиться входная фильтрация потока сообщений, выделение данных, адресованных конкретным абонентам (с помощью априорно известных или экспериментально определенных кеп-кодов). Возможно осуществление поиска, распечатки и русификации перехваченных сообщений.
Как и в обычной телефонной сети, здесь тоже предусмотрен государственный контроль, который организован следующим образом. Министерство связи России обязало всех операторов мобильной телефонной и пейджинговой связи обеспечить доступ российских спецслужб к своим сетям. Эти требования сформулированы в приказе Минсвязи № 9 от 31 января 1999 года «Об организации работ по обеспечению оперативно-розыскных мероприятий на сетях подвижной связи». В соответствии с техническим приложением к приказу система предназначена «для оперативного контроля соединений и местоположения определенных пользователей оперативной связи». То есть с ее помощью можно не только прослушивать разговоры, но и определять местоположение абонента телефона, даже если по нему не ведется разговор. Предусматривается создание баз данных передаваемой по мобильным сетям информации и точных адресов пользователей. Приказ также подразумевает контроль за всеми номерами, на которые переадресуется вызов, и всеми дополнительными услугами, предоставляемыми абонентам операторами мобильной связи. В документе расписаны виды, методы контроля, а также способы защиты информации от несанкционированного доступа.
Значительно более сложной задачей является перехват междугородных телефонных переговоров, ведущихся с привлечением радиорелейных линий связи. Используемые в России радиорелейные линии являются многоканальными системами передачи (до 3600 каналов), что усложняет задачу съема. Расстояние от радиорелейной станции, с которого возможно осуществление перехвата информации, совсем невелико, так как передающая антенна имеет узкую диаграмму направленности. Впрочем, можно располагаться вблизи приемного (передающего) пункта либо вдоль линии трассы в главном лепестке антенны. Комплект для перехвата информации с микроволновых линий связи включает:
>• параболические антенны (2 шт) ..... 1000 $;
>• радиоприемники с частотными демодуляторами (2 шт) ..... 10 000$;
>• демодуляторы, соответствующие полосе модулирующих частот (2 шт)..... 10 000$;
>• управляющий процессор со сканированием ..... 1000 $;
>• осциляторы с цифровой настройкой (2 шт) ..... 700 $;
>• устройство декодирования сигналов вызова (2 шт)..... 1500 $;
>• смеситель..... 50 $;
>• магнитофон..... 100 $.
Таким образом, полная стоимость подобного комплекта приближается к 40

тысячам $, что делает его совсем непривлекательным для рядовых шпионов. Хотя, в принципе, могут быть использованы типовые разведывательные приемники с дополнительными выходными устройствами разуплотнения и демодуляции принимаемых сигналов. В приемном устройстве многоканальный сигнал селектируется, детектируется и усиливается до уровня, достаточного для нормальной работы записывающих устройств. При этом к системе предъявляются жесткие требования по стабильности частоты, нелинейным искажениям и появлению комбинационных частот.

В качестве примера рассмотрим систему **РК445**, предназначенную для перехвата телефонных переговоров, факсимильных сообщений и т. д. Диапазон рабочих частот — 0,1...18,5 ГГц. Точность настройки — 100 Гц. Возможно детектирование сигналов с АМ, ЧМ и импульсной модуляцией. Перехваченные сигналы снабжаются меткой времени с датой и могут быть записаны на встроенный магнитофон либо распечатываться на принтере. Управление системой осуществляется с ноутбука 486 SL25.

Серьезные задачи под силу организациям типа национального АНБ. Эта правительственная организация насчитывает в 6 раз больше служащих, чем ЦРУ. Она занимается электронной разведкой, причем на ее долю приходится большая часть американских ассигнований на нужды разведки. Имеется 4120 мощных центров прослушивания, размещенных на многочисленных военных базах в Германии, Турции, Японии и других странах, а также на борту американских кораблей, подводных лодок и самолетов.

АНБ имеет возможность собирать и анализировать почти повсеместно радиограммы, телефонные переговоры, идущие по радиорелейным и спутниковым каналам связи, электронные сигналы любого типа, включая излучения систем сигнализации в квартирах и противоугонных устройств автомобилей. Достаточно сказать, что агентство ежедневно «перерабатывает» до 40 т секретной документации.

Аналогичной деятельностью занимается британский Штаб правительственной связи (ШПС). У АНБ и ШПС имеется список лиц и организаций, все переговоры которых перехватываются автоматически. Этот список включает в себя ряд нефтяных компаний, банков, газет, имена известных дилеров на товарных рынках и лидеров ряда политических и общественных организаций. Для обработки перехваченной информации используются быстродействующие компьютеры, которые ведут поиск ключевых слов со скоростью до 4 млн знаков в секунду. Это означает, что они способны прочитать среднюю по объему газету быстрее, чем человек пробежит глазами ее заголовок. Когда компьютер наталкивается на определенное слово, означающее, что данный текст представляет интерес для АНБ или ШПС, изготовляется его печатная копия для дальнейшего изучения, причем тексты распечатываются устройствами, выдающими 22 тысячи строк в минуту. Таким образом, информация о событии, сообщении или переговорах, представляющих особое политическое или военное значение и называемых на специальном языке «критическими», ляжет на стол президента США в среднем через 10 минут.

Участники международных проектов вполне могут стать объектом внимания спецслужб, часто действующих в интересах национальных корпораций. Действительно, как отмечает западная печать, американская радиоразведка, которая становится «свидетелем» многих коммерческих сделок, в состоянии выявить «узкие места» в развитии экономики многих стран, в том числе и России. Известно, например, что АНБ получило большие дивиденды, осуществляя перехват сообщений газовых и нефтяных компаний на Ближнем Востоке, финансовых и торговых организаций в Европе и Японии и передавая эту информацию американским фирмам. По некоторым данным, перед АНБ ставятся задачи о целенаправленном контроле за конкретными компаниями.

К зоне Е возможно отнести и сравнительно молодой вид связи — уникальную систему действующей в России внутригосударственной спутниковой связи с

разветвленной сетью наземных станций «Орбита», «Экран», «Москва». Через спутники «Горизонт» вместе со спутниками «Молния-3» и «Радуга» обеспечивается телефонная и телеграфная связь по территории всей страны. Большинство спутниковых линий связи использует диапазон 4...6 ГГЦ. Интересно, что в ФРГ в свое время в законе о борьбе с преступностью предусматривалась возможность подслушивания международных телефонных переговоров именно по спутниковым каналам связи.

Даже в проект системы глобальной спутниковой связи для мобильных абонентов **Indium** (инициирован фирмой Motorola) Центр им. Хруничева по настоянию Минсвязи согласился внести некоторые коррективы. В частности, был определен четкий порядок размещения в будущей сети аппаратуры спецслужб, чтобы они без труда могли проводить так называемые оперативно-розыскные мероприятия.

Группа радиоэлектронного контроля (Франция) имеет в своем распоряжении около 100 технических постов, в том числе за рубежом, и ведет перехват информации радиоэлектронными средствами, а также обеспечивает прослушивание телефонных переговоров. При этом в последние годы руководители Франции настойчиво говорят о важности усиления разведывательной деятельности именно в экономической области, подчеркивая особое значение обеспечения экономических интересов в условиях острой конкурентной борьбы с другими странами.

Таким образом, практически все страны мира контролируют телефонные переговоры в зоне Е (по крайней мере, имеют такую возможность при необходимости).

Для перехвата сообщений по космическим каналам связи также могут использоваться спутники-разведчики. Первые спутники радиоэлектронной разведки, вероятно, запускались в конце 60 — начале 70-х годов. Известно, что первый спутник типа **Rhyolit** вышел на орбиту в марте 1973 года. В 1979 и в 1981 годах были запущены два усовершенствованных спутника радиоэлектронной разведки **Shalet.** В 1985 году был запущен спутник типа **Magnum.** Запуск космических аппаратов продолжался с помощью многоразовых аппаратов типа «Шатл». В качестве примера современного космического разведчика можно описать спутник **«Аквакейд»,** осуществляющий прослушивание каналов радиосвязи в диапазоне частот 0,5...40 000 МГц. Спутник имеет две параболические антенны диаметром около 23 м и обладает весьма высокой чувствительностью и точностью привязки обнаруженного излучения объекта к местности. Он перехватывает от 300 до 3000 каналов связи одновременно и через спутники-ретрансляторы типа TDRSS передает информацию на наземные пункты, где проводится демодуляция сигналов и определение с помощью ЭВМ по дескрипторным словам тех сообщений, которые представляют интерес для спецслужб. Особое внимание уделяется перехваченным частным разговорам.

Спутники радиоразведки стоят порядка 300 млн $ и выводятся на геостационарные орбиты. Они предназначены для перехвата переговоров как по военным и дипломатическим каналам радиосвязи, так и по каналам, имеющим коммерческое значение. Группировка спутников радиоэлектронной разведки обычно состоит из 10...20 аппаратов, а 5...6 из них постоянно ведут перехват информации с радиорелейных, тропосферных, спутниковых и других линий связи. Эта информация также может быть передана заинтересованным организациям, имеющим бизнес в России.

Таким образом, существуют десятки методов и средств перехвата информации, циркулирующей в телефонной сети. В связи с этим представляет существенный интерес анализ возможности сохранения конфиденциальности сообщений от частных компаний.

Чтобы оценить реальные возможности крупных фирм, приведем небольшой пример. 13 июля 1982 года АНБ перехватило направленное в Японию коммерческое сообщение из представительства компании «Мицубиси» в

Вашингтоне. Наличие у «Мицубиси» подробной факсимильной информации из совершенно секретных разведывательных сводок от 7 и 9 июля вызвало у ФБР большую тревогу... В перехваченном АНБ 29 июля 1982 года втором сообщении японской компании давались обширные цитаты из национальной разведывательной сводки от 26 июля.

### 1.5.2. Методы и средства несанкционированного получения информации в каналах сотовой связи

В ближайшее время во всем мире радиосвязь станет обычным атрибутом жизни. Эта тенденция, являющаяся следствием научно-технической революции в коммерческой связи, по мнению одних экспертов, может дать существенные преимущества службам разведки, а по мнению других — приведет к новым запретам на проведение мероприятий по прослушиванию и перехвату информации. Вероятно, в определенной мере правы и те, и другие.

Подвижная сотовая радиотелефонная система является в настоящее время наиболее интенсивно развивающимся видом связи. Не случайно она занимает ведущее место на рынке массовых услуг. Но радиотелефонная связь (а сотовая в особенности) более уязвима к действиям злоумышленников, чем традиционная телефонная связь по проводным линиям.

Лавинообразный рост количества действующих радиосетей создает новые возможности для добывания конфиденциальной информации. Эти возможности еще более расширятся после утверждения и внедрения стандартов на цифровую сотовую радиосвязь и переходу к более широкому применению этого вида связи в развивающихся странах. В настоящее время по сетям радиосвязи во всем мире передаются миллионы телефонных разговоров и это количество будет только возрастать.

Съем информации из сетей сотовой радиосвязи может представлять задачу различной степени трудности в зависимости от того, какие цели ставят перед собой перехватчики и от типа контролируемых сетей. Перехватчик-любитель будет упорно сканировать диапазон частот сотовой системы в надежде наткнуться на случайный разговор, представляющий для него интерес. Он легко найдет необходимую для этого аппаратуру на местном радиоэлектронном рынке. Для ведомств типа АНБ США, заинтересованных в мониторинге всего трафика в сетях сотовой радиосвязи, например, в зонах больших городов, с целью выявления информации об определенных организациях или объектах, потребуется более сложная аппаратура, сведения о которой, как правило, не публикуются в открытой печати. Чтобы лучше понять принцип действия такой аппаратуры, рассмотрим работу системы мобильной связи более подробно.

Типовая сотовая радиотелефонная сеть состоит из трех основных компонентов: коммутационного центра MTSO (Mobile Telephone Switching Office), системы базовых станций и подвижных сотовых радиотелефонов (или радиотелефонных станций).

Коммутационный центр является мозгом сети. Его главный компьютер управляет сотнями тысяч соединений в зоне, обслуживаемой данным центром. Центр MTSO назначает частоты для радиосвязи базовым станциям и подвижным радиотелефонам, а также распределяет вызовы в пределах своей зоны между сотовой сетью и обычными телефонными станциями общего пользования. Базы данных сотовой сети содержат информацию как о местонахождении всех ее клиентов, так и об интерфейсах с другими такими же сетями, что необходимо для идентификации абонентов и проверки их права на доступ в сеть.

Каждая базовая станция представляет собой контроллер, соединяющий ее через интерфейсы проводных линий с несколькими сотовыми радиопередатчиками (передатчиками отдельных сот). Это передатчики относительно небольшой мощности (не более 100 Вт) с антеннами, монтируемыми на стальных мачтах высотой до 30 м. Сотовые передатчики

работают в диапазоне частот 430...1900 МГц (в зависимости от типа сети и страны, где она расположена) и позволяют вступить в связь в пределах прямой видимости с подвижными радиотелефонами. Обычно радиус зоны, обслуживаемой одним сотовым радиопередатчиком, не превышает 20 км. Зоны сотовых радиопередатчиков перекрываются для обеспечения непрерывной связи с абонентами при его перемещении в пределах всего района обслуживания. Таким образом, главное отличие от обычных радиостанций, мощные передатчики которых позволяют организовать вещание на весьма ограниченных территориях, заключается в том, что в сотовых сетях большая территория разделяется на определенное количество малых, но взаимодействующих ячеек (сот). Различные сотовые сети могут соединяться между собой для перекрытия еще больших районов, а в перспективе даже всей территории страны.

В принципе, центры MTSO назначают соседним сотовым радиопередатчикам строго определенные поддиапазоны из общего диапазона частот. Но в районах с большей плотностью населения, например, городских, количество пользователей сотовыми радиотелефонами может в любое время превысить потенциальные возможности сети. Чтобы избежать такой опасности, сотовая система должна применять повторное использование рабочих частот и распределять их между отдельными сотами в соответствии с общей конфигурацией сети. В районах интенсивного телефонного трафика поставщики услуг сотовой связи вынуждены использовать в сети большее количество сот меньших размеров, чем это необходимо для «состыковки» границ участков, что практически означает увеличение числа доступных каналов связи. Необходимое условие при таком подходе к построению сети состоит в том, чтобы соты, использующие одинаковые рабочие частоты, были разделены географически возможно большими расстояниями во избежание межканальных помех, возникающих когда подвижная станция одновременно принимает сигналы от двух сотовых передатчиков. Это значит, что ни при каких условиях одинаковые рабочие частоты не могут назначаться соседним сотам, поэтому при их смене может произойти сбой связи. Во избежание таких ситуаций в сотовых сетях применяется так называемый режим handoff — принятие решения о переключении частоты подвижного абонента при его перемещении из одной соты в другую.

Именно режим handoff, который можно назвать «медленной скачкообразной перестройкой рабочей частоты» (slow frequency hopping) и специальный протокол управления сетями превращают сотовую связь в довольно сложный для радиоразведки объект, более сложный, чем любые другие виды радиосвязи.

Основной зоной ведения радиоразведки в сотовых сетях является воздушный интерфейс, или участок между мачтой, на которой установлена антенна радиопередатчика, и движущимся радиотелефоном. Это обычно единственное открытое соединение в сети, а следовательно, и единственный сегмент системы, где имеет смысл осуществлять перехват сигналов для определения местоположения (радиопеленгации) радиопередатчика. Но сам по себе перехват сигналов не является основной трудностью для радиоразведки, так как большинство действующих в настоящее время сотовых сетей — это аналоговые системы, соответствующие стандартам AMPS, TACS, NMT—450i. Для передачи в этих сетях обычно используются ЧМ-сигналы, перехват которых легко осуществить, используя для этого сканирующий радиоприемник с ЧМ-демодулятором. Вместе с тем, простой перехват радиосигналов не решает основных задач для радиоразведки. Например, даже радиолюбитель с приемником указанного типа может прослушивать случайно перехваченные переговоры в сотовой сети. Но он не сможет следить за этими переговорами при передвижении мобильного радиотелефона из одной соты в другую, а значит и переходе с одной частоты на другую. Для этого требуется значительно более сложная техника, например, с

использованием специальных методов демодуляции с четким выделением сигналов управления перестройкой частоты радиотелефона при переходе его из одной соты в другую.
В принципе, располагая несколькими сотовыми телефонами, компьютером и приобретя необходимые дополнительные компоненты, злоумышленник, имеющий некоторые технические знания, может сконструировать прибор, дающий ему возможность следить за радиотелефоном в соседней соте и перехватывать входящие и исходящие вызовы и разговоры. При каждом вызове такое устройство может автоматически соединяться с аудиомагнитофоном.
Для слежения за частотными переходами мобильного радиотелефона нужны по существу два радиоприемника: один для перехвата аудиоинформации и второй для выделения сигналов управления, например, с использованием демодулятора с частотным сдвигом.
Основной способ, которым пользуются заинтересованные лица для создания аппаратуры указанного типа, состоит в использовании модификации модема с платами PCMIA. Производится небольшая перенастройка модема, подключенного к сотовому телефону, в область более низких частот относительно несущей частоты передачи речевой информации, то есть в сторону частот, на которых осуществляется передача сигналов управления. Программные средства для управления такой перестройкой общедоступны через сеть Интернет. Если соединить модифицированный модем с персональным компьютером, то можно получить на экране дисплея сигналы управления перестройкой частоты радиотелефона при его переходе из исходной соты сети в соседнюю, коды управления и информацию, относящуюся к вопросам безопасности сети. При этом модем преобразует перехваченную речь в цифровую форму и выводит ее для записи на жесткий магнитный диск, то есть злоумышленнику даже не требуется магнитофона. Как видите, неуязвимая, если верить рекламе, сотовая связь вполне доступна даже грамотному любителю.
Однако профессионал никогда не будет пользоваться такой примитивной методикой, поскольку определенные шаги в направлении развития и совершенствования специальной техники предпринимают фирмы, производящие аппаратуру радиоразведки. Рынок насыщен техническими средствами перехвата, мониторинга и радиопеленгации в сетях сотовой радиотелефонной связи. Ажиотаж в области коммерческой сотовой радиосвязи безусловно способствовал и расширению производства средств радиоразведки в этих сетях. К известным фирмам, поставщикам военной аппаратуры радиоразведки (AST, Rockwell, Rhodes, Thomson, Marconi, Rafael, Watking-Johhsons и др.), присоединился еще целый ряд организаций, в том числе российских, клиентами которых являются правоохранительные органы и сами компании, оказывающие услуги по организации сотовой радиотелефонной связи. Используя преимущества коммерчески доступных программных средств и техники цифровой обработки сигналов, удалось создать системы с размерами атташе-кейса, которые способны одновременно контролировать несколько каналов.
Например, фирма Law Enforcement Equipment Corp. рекламирует систему перехвата переговоров сотовых радиотелефонов **Cellular Telephone Monitoring System**, контролирующую 19 каналов и фиксирующую разговоры по трем каналам одновременно. Канадская фирма Electronic Counter-measures предлагает систему **Cellular Analysis System 8000**, управляемую персональным компьютером и имеющую размеры атташе-кейса, способную использовать до 24 приемников для мониторинга каналов передачи речевой информации и сигналов управления в сотовых сетях, соответствующих стандартам AMPS и D-AMPS (новая версия стандарта AMPS для сотовых сетей).
Для заказчиков с более строгими требованиями к аппаратуре радиоразведки перечисленные выше крупные фирмы-поставщики военной электроники

предлагают новые системы радиоразведки в сетях сотовой связи. Хорошей иллюстрацией их реальных возможностей является стандартная многоканальная система **Model 1235 Multichannel Digital Receiving System** фирмы AST. Она имеет 60 независимых цифровых радиоприемников с переключаемыми демодуляторами частотно-модулированных сигналов (обычных при передаче речевой информации) и частотно-манипулированных сигналов (цифровых сигналов управления), а также (если это требуется) демодуляторов сигналов с другими видами модуляции. В этой очень эффективной системе используются сдвоенные процессоры цифровых сигналов фирмы Texas Instruments, выполняющие обработку самыми современными программными средствами. Этим обеспечивается высокая гибкость режимов, что позволяет успешно применять ее и в сотовых сетях, использующих новые стандарты (если они будут приняты).

Созданы и более мощные системы перехвата информации и радиопеленгации в сетях сотовой радиотелефонной связи, контролирующие множество каналов в радиусе до 350 км, но операторы этих систем встречаются с определенными трудностями. Главная из которых, как это не парадоксально, вызвана широким распространением аппаратуры сотовой связи.

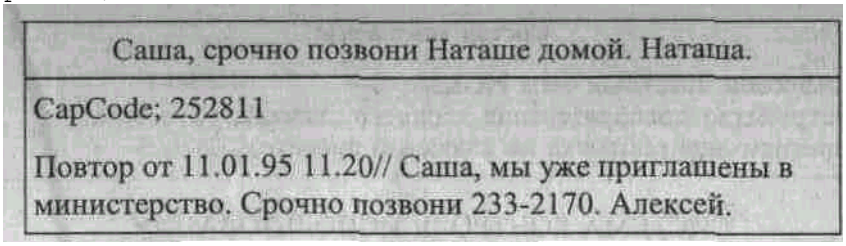
Сейчас проще перечислить страны, в которых мобильный телефон еще не применяется, чем страны, где он уже используется в полной мере. Только в США у пользователей находится более 50 сотовых радиотелефонов на тысячу жителей. Обнаружение и выделение нужных сигналов, представляющих интерес,— очень сложная задача, так как все абоненты сотовых сетей пользуются одинаковыми радиотелефонами фирм Motorola, Ericsson, Nokia. Передаваемые ими сигналы смешиваются в общем графике очень больших гражданских сотовых сетей. Так как станции применяют принципы повторного использования радиочастот (если они не соседи), то пункт радиоразведки будет наводнен множеством сигналов, частоты которых будут совпадать, что крайне затруднит как мониторинг, так и радиопеленгацию.

Но ряд фирм, поставщиков аппаратуры радиоразведки, уже смогли найти решение и этой проблемы. Так компания AST предлагает различные системы с адаптивным формированием диаграммы направленности приемных антенн и схемами подавления помех. Израильская фирма Rafael Electronic System Division разработала радиопеленгационную систему со сверхвысоким разрешением, и хотя не рекламирует ее как систему для мониторинга сотовой связи, но для специалиста вопрос очевиден. Из сказанного видно, что глобальный контроль мобильной связи вполне реален даже при современном уровне развития техники.

Традиционные аналоговые системы сотовой связи хотя и могут создавать определенные трудности для радиоразведки, но не считаются «крутыми» противниками. Более серьезные опасения у этой службы вызывает предстоящий массовый переход на цифровые системы. Уже разработаны и внедряются стандарты на цифровые сотовые радиотелефоны: Digital AMPS (США, Россия), GSM или Global System for Mobile Communication (Западная Европа, Россия), NTT (Япония). Новую аппаратуру более правильно называть системами персональной связи PCS (Personal Communication System), так как она может быть использована также для пейджинговой связи и передачи данных.

Хотя системы сотовой цифровой радиосвязи работают в том же диапазоне радиочастот, что и действующие в настоящее время традиционные аналоговые системы, в них применяются более сложные сигналы и, самое главное, они имеют встроенные средства защиты информации, например, криптографические. Три действующих стандарта на системы цифровой сотовой радиосвязи предусматривают применение многократного доступа с временным разделением TDMA, означающего возможность одновременной передачи трех разговоров по одному каналу с последовательным разделением их передачи во времени (что эквивалентно одному вызову).

Это в три раза затрудняет ведение радиоразведки.
Другой стандарт цифровой сотовой радиосвязи с использованием многократного Доступа с кодовым разделением CDMA дает возможность применения техники широкополосных систем с малой вероятностью обнаружения сигналов. Практически никакие другие системы связи не представляют таких трудностей для ведения радиоразведки, как широкополосные, но это уже тема для другой книги.
В заключение раздела познакомьтесь с возможностями некоторых типов аппаратуры, выпускаемой серийно и вполне доступной для заинтересованных лиц.
КОМПЛЕКС ПЕРЕХВАТА ПЕЙДЖИНГОВЫХ СООБЩЕНИЙ СТАНДАРТА POCSAG PAGER RESEPT 2.1
**Назначение:**
для приема и регистрации на жестком диске ПЭВМ текстовых и цифровых сообщений в действующих в настоящее время системах радиопейджинга стандарта POCSAG.
Комплекс производит мониторинг радиопейджинговых систем Vessolinfe «Телекомт», «Радиопедж», «Информ», «Экском», «Мадти Пейдж», «Моторола мобайл коммуникейшинз», «Радиопоиск», «Ростехэкспорт» и др.
**Комплекс обеспечивает:**
**>•** прием и декодирование текстовых и цифровых сообщений, передаваемых в системах редиопейджинговой связи. Сохранение всех принятых сообщений на жестком диске в архивном файле;
**>•** входную фильтрацию общего потока сообщений, выделение данных, адресованных одному или ряду конкретных абонентов по априорно известным или экспериментально определенным кеп-кодам, оперативное изменение состава контролируемых абонентов;
**>•** входную русификацию (для русифицированных пейджеров) всего потока сообщений, адресованных только конкретным абонентам, включенным в список наблюдаемых;
**>•** обработку файлов выходных данных в любом текстовом редакторе с реализацией стандартной функции поиска по введенной строке символов и печатью необходимых данных на принтере.
**Основные режимы работы:**
**>•** все сообщения только на экран — принимаемые сообщения выводятся на экран без сохранения на жестком диске;
**>•** все сообщения на экран и в архив — все, что выводится на экран, сохраняется на жестком диске;
**>•** на экран — только наблюдаемые, а в архив — все сообщения (по смыслу режима).




**Вид экрана ПЭВМ в режиме ВСЕ СООБЩЕНИЯ НА ЭКРАН И В АРХИВ**
**Состав комплекса:**
**>•** доработанный сканирующий приемник типа AR-3000A, Radio-Shack, IC-R7100 или им аналогичный;
**>•** устройство преобразования входного сигнала;
**>•** программная оболочка Pager Recept входного сигнала;
**>•** персональный компьютер.
КОМПЛЕКС ПЕРЕХВАТА ПЕЙДЖИНГОВЫХ СООБЩЕНИЙ СТАНДАРТА RDS
**Назначение:**

для приема регистрации на жестком диске ПЭВМ текстовых и цифровых сообщений в действующих в настоящее время на территории России системах радиопейджинга стандарта RDS (группа 7А).

**Комплекс обеспечивает:**

>• прием и декодирование текстовых и цифровых сообщений, передаваемых в системах радиопейджинговой связи RDS;

>• сохранение всех принятых сообщений на жестком диске в архивном файле;

>• фильтрацию общего потока сообщений, выделение данных, адресованных одному или ряду конкретных абонентов по априорно известным или экспериментально определенным кеп-кодам, оперативное изменение параметров списка наблюдаемых абонентов;

>• входную русификацию всего потока сообщений или адресованных только конкретным абонентам, включенным в список наблюдаемых;

>• обработку файлов входных данных в любом текстовом редакторе с реализацией необходимых данных на принтере.

**Состав комплекса:**

>• цифровой приемник типа NOKIA;

>• устройство преобразования входного сигнала;

>• программная оболочка на ключевой дискете.

СИСТЕМА КОНТРОЛЯ ИСПОЛЬЗОВАНИЯ СЛУЖЕБНЫХ РАДИОТЕЛЕФОНОВ СОТОВОЙ СВЯЗИ СТАНДАРТА NMT-450 ТСС-1

**Назначение:**

для контроля использования мобильных телефонов абонентами систем сотовой связи стандарта NMT-450L

Система позволяет обнаруживать и сопровождать по частоте входящие и исходящие звонки абонентов связи, определять входящие и исходящие номера телефонов абонентов, осуществлять слежение по частоте за каналом во время телефонного разговора, в том числе при переходе из соты в соту.

Система дает возможность одновременно с контролем осуществлять автоматическую запись переговоров на диктофон, вести на жестком диске ПЭВМ протокол записей на диктофон, осуществлять полный мониторинг всех сообщений, передаваемых по служебному каналу, а также определять радиослышимость всех базовых станций в точке из приема с ранжировкой по уровням принимаемых от базовых станций сигналов.

**Основные режимы работы:**

база—мобильный — слежение по выбранной базовой станции за всеми входящими звонками на мобильные телефоны со стороны АТС или за звонками только на те телефоны, номера которых предварительно заданы:

мобильный—база — слежение по выбранной базовой станции на частоте базовой станции за всеми исходящими звонками владельцев мобильных телефонов или за звонками только с тех телефонов, номера которых предварительно заданы. В процессе слежения определяются номера телефонов, с которых звонят, и телефонов, куда звонят;

мобильный — слежение по выбранной базовой станции на частотах мобильных телефонов за всеми исходящими звонками владельцев мобильных телефонов или звонками только с тех телефонов, номера которых предварительно заданы;

приемник — контроль переговоров на частотных каналах выбранной базовой станции. В процессе контроля возможна запись ведущихся переговоров на диктофон и слежение по частоте за переговорами выбранного абонента при переходе абонента из одной соты в другую;

Город- Москва 14:44:46 Вызов телефона 901-4626 /Город- Москва 14:44:46 Вызов телефона 901-4626

Город- Москва 14:44:46 Вызов телефона 902-5060 /Город- Москва

14:44:46 Вызов телефона 901-5168

**Вид экранного меню в режиме БАЗА—МОБИЛЬНЫЙ**

диктофон — прослушивание записанных на диктофон переговоров по каналам сотовой связи. При наличии в записи цифрового обмена между мобильным телефоном и базовой станцией возможно определение номера телефона, разговор с которого был записан на диктофон;

базы — автоматическое определение базовых станций, по которым может вестись в данной точке приема контроль переговоров.

**Технические характеристики:**

>• максимальное количество задаваемых для контроля телефонных номеров: 100;

>• максимальное количество базовых станций, по которым возможно одновременное осуществление контроля за звонками и переговорами: 2.

**Состав аппаратуры:**

>• ПЭВМ класса PC AT 486-66МГц/4Мб и выше (в базовый комплект поставки не входит);

>• плата обработки сигналов, встраиваемая в ПЭВМ;

>• два радиоприемника AR-3000A со скоростью приема/передачи данных 9600 бод (в базовый комплект поставки не входит);

>• специальное программное обеспечение;

>• комплект соединительных кабелей.

По желанию заказчика система может быть выполнена в одноканальным переносном варианте с использованием ПЭВМ типа Notebook и возможностью записи переговоров на жесткий диск.

КОМПЛЕКС ПЕРЕХВАТА СОТОВОЙ СВЯЗИ

**Назначение:**

для контроля использования служебных телефонов сотовой связи стандарта AMPS.

Система позволяет обнаруживать и сопровождать входящие и исходящие звонки телефонов сотовой связи, а также определять номера телефонов сотовой связи.

**Режимы работы:**

базовая станция—мобильный телефон — контроль звонков на мобильный телефон со стороны АТС;

мобильный телефон—базовая станция — контроль звонков владельцев мобильных телефонов через АТС. В этом режиме возможно определение номера не только абонента сотовой сети, но и номера телефона, куда производится звонок.

Данная система одноканальная, поэтому слежение и контроль осуществляется по одному из каналов — входящие звонки («базовая станция») на частотах одной базовой станции.

Система позволяет одновременно с контролем производить автоматическую запись разговора на диктофон, а также осуществлять автоматический выбор базовой станции, обеспечивающей Оптимальный прием переговоров.

Конструктивно система размещена в кейсе.

**Технические характеристики:**

>• максимальное количество задаваемых для контроля телефонных номеров: 16.

**Состав системы;**

>• ПЭВМ класса PC AT 486—66МГц/4Мб и выше (в базовый комплект поставки не входит, поставляется дополнительно по требованию заказчика);

>• блок декодеров прямого и обратного каналов;

>• доработанный сканирующий радиоприемник AR-3000A;

>• диктофон Sony;

>• программное обеспечение;

>• соединительные кабели.

СИСТЕМА КОНТРОЛЯ СОТОВОЙ СВЯЗИ

**Назначение:**
для контроля правил ведения переговоров в аналоговой и цифровой сотовой системе связи стандарта DAMPS («БиЛайн» в г. Москве) в пределах зоны действия выбранной соты и регистрации содержания ведущихся переговоров на магнитный носитель.
Система изготовлена на основе цифро-аналоговой телефонной трубки и является одноканальной.
**Система обеспечивает:**
>• контроль входящих и исходящих звонков конкретных абонентов сотовой системы связи, включенных в список наблюдаемых, либо выборочный контроль переговоров произвольных абонентов;
>• контроль дуплексного радиоканала при условии радиодоступности мобильного абонента;
>• слежение за разговором при переходе абонента из одной соты в другую при условии радиодоступности новой соты;
>• регистрацию содержания ведущихся переговоров с использованием внешнего записывающего устройства.
**Основные режимы работы:**
>• сопровождение одного из заданных телефонных номеров — ввод требуемых номеров производится с клавиатуры. При нахождении с контролируемым абонентом в одной соте система обеспечивает обнаружение входящих и исходящих звонков, автоматически переключается на выделенный для абонента речевой канал, осуществляет слуховой контроль ведущихся переговоров независимо от типа выделенного речевого канала (аналоговый или цифровой) и производит сопровождение разговора при смене канала (например, при переходе на частоту другой соты). Слуховой контроль осуществляется на частоте базовой станции. Номера фиксируемых звонков запоминаются в оперативной памяти трубки с возможностью их просмотра в режиме «прокрутки»;
>• автоматизированный сквозной контроль сообщений — в этом режиме осуществляется последовательный слуховой контроль произвольных абонентов. Система в автоматическом режиме определяет оптимальный канал контроля для выбранного места проведения работ. После фиксации первого же разговора система автоматически настраивается на выделенный речевой канал и сопровождает разговор (в том числе при переходе из соты в соту) либо до его завершения, либо до прерывания оператором. После этого система возвращается на оптимальный в данный момент времени и в данном месте служебный канал. Номера фиксируемых звонков запоминаются в оперативной памяти трубки;
>• ручной сквозной контроль сообщений — от второго режима отличается лишь выбором контролируемого канала оператором в ручном режиме и является вспомогательным. Подключение внешнего устройства магнитной записи осуществляется через 3,5-мм стандартный телефонный разъем.
**Технические характеристики:**
>• максимальное количество задаваемых для наблюдения абонентов: 16 (в зависимости от версии программного обеспечения количество наблюдаемых абонентов может меняться в сторону увеличения).

## 1.6. Получение информации, обрабатываемой в компьютерных сетях

### 1.6.1. Основные способы несанкционированного доступа

Изобретение компьютера дало людям уникальный инструмент, который существенно раздвинул границы человеческих возможностей. Вычислительным

машинам стали доверять многие секреты, используя ЭВМ как средство хранения, обработки и передачи информации.
В свою очередь, это повлекло к увеличению уязвимости информации от преднамеренных или случайных воздействий и даже породило новый вид преступлений — компьютерные преступления.
Так например, в ноябре 1998 года Нагатинский суд Москвы завершил первый в России процесс над хакером — 18-летним студентом Московского института радиоэлектроники и автоматики Павлом Шейко. Этот компьютерный пират на скамью подсудимых попал за то, что, используя фиктивные кредитные карты компании American Express, заказал в техасском магазине PC Teach (США) через компьютерную сеть Internet товары (главным образом компьютеры и их компоненты) на сумму более 20 тысяч $, и даже умудрился получить их и частично реализовать. Рассчитывал Шейко, главным образом на то, что его не станут разыскивать за мелкую кражу, тем более на территории другой страны.
Другой мошенник — сотрудник вычислительного центра Миллеровского отделения Ростовского Сбербанка 32-летний Сергей Пахмутов. В феврале 1999 года был осужден по статье 273 УК РФ «Создание, использование и распространение вредоносных программ для ЭВМ» на два года лишения свободы условно. Он разработал и запустил в компьютерной сети Сбербанка программу, которая должна была во всех 900 филиалах открыть счета на вымышленное имя и перечислить на них несколько десятков миллионов рублей. Преступление было остановлено благодаря собственной службе безопасности Сбербанка, которая выявила прохождение несанкционированной программы, блокировала фиктивные счета и, проведя служебное расследование, выявила авантюриста.
Однако наиболее скандальная известность среди российских хакеров принадлежит Владимиру Левину, которого в 1995 году арестовали британские спецслужбы по обвинению в краже денег из американского Citibank. Аферу с банком Левин провернул летом 1994 года, подключившись к компьютерной сети Citibank и взломав ее защиту. После этого он перевел круглую сумму со счетов клиентов банка своим сообщникам. Служба безопасности банка проследила пути следования денег, и когда кто-либо из сообщников пытался снять деньги, его тут же арестовывали. Всего по делу Левина проходило пять человек, сам он приговорен судом США к трем годам тюрьмы.
Для предупреждения подобных и целого ряда других преступлений, связанных с воздействием на вычислительные средства, стали разрабатываться различные, в том числе и достаточно сложные (многоуровневые) системы защиты.
Преодоление этих систем с целью получения доступа к защищенной информации, хранящейся и обрабатываемой в компьютерных системах, — одна из задач людей, которые занимаются промышленным шпионажем.
Под основными способами несанкционированного доступа к компьютерной информации обычно понимают следующие:
- преодоление программных средств защиты;
- несанкционированное копирование информации;
- перехват информации в каналах связи;
- внедрение программных закладок и компьютерных вирусов;
- использование аппаратных закладок;
- перехват побочных электромагнитных излучений и наводок (ПЭМИН), а также некоторые другие.

Естественно, что такое деление является в значительной степени условным (как, впрочем, и любая классификация), так как практически каждый из приведенных способов может в определенных случаях выступать составной частью любого другого из перечисленных.
Но все же, под преодолением программных средств защиты обычно понимают

применение различных методов взлома, использующих слабые места преодолеваемых систем. В п. 1.6.2 и 1.6.3 они будут рассмотрены подробнее.

Несанкционированное копирование информации подразумевает копирование с дискет и жестких дисков, к которым возможен случайный или подготовленный доступ. Иногда копирование с жесткого диска применяется как способ обхода систем защиты, не использующих кодирование хранящейся информации. С этой целью вскрывается системный блок, извлекается жесткий диск, который подключается к другому компьютеру, например через SCASY — адаптер. После чего с него переписывается вся необходимая информация и жесткий диск возвращается на место.

Особо следует отметить возможность копирования файлов, удаленных законным пользователем. Дело в том, что при удалении файл на самом деле не уничтожается, а удаляется только его имя из таблицы размещения файлов, содержание же файла остается на диске и затирается естественным путем по мере осуществления новых записей. Для поиска и восстановления еще не «затертых» файлов можно воспользоваться специальными Нортон-утилитами (Norton Utilities), типа QU или UnErase Wizard, которые имеются практически на любом загрузочном компакт-диске. Такие утилиты позволяют осуществлять поиск и восстановления файлов по имени, времени удаления и даже по ключевым словам. После восстановления файл может быть скопирован на дискету, но затем должен быть вновь удален с целью скрытия факта восстановления.

Необходимо отметить, что некоторые компьютерные системы защиты информации предусматривают гарантированное удаление файлов, например, путем трехкратной записи единиц на освободившееся место. Таким свойством обладает программно-аппаратная система **Dallas Lock3.1**, которая будет рассмотрена в п. 2.6.4. Естественно, что восстановление и последующее копирование файлов становится после этого невозможным.

Способы перехвата информации в каналах связи аналогичны рассмотренным в п. 1.5. Причем, перехват возможен не только в проводных, но и в радиоканалах, так как из-за быстрого внедрения в повседневную жизнь систем мобильной связи, использование радиомодемов уже перестало быть экзотическим событием.

Использование программных закладок позволяет решать задачи как перехвата конфиденциальной информации с копированием ее в заранее обусловленное место, так и задачи взлома систем защиты, например, для перехвата паролей (п. 1.6.3). Программные закладки обычно маскируются внутри других программных продуктов, и по принципу действия попадают в разряд программ, известных под названием троянского коня, по аналогии с идеей, блестяще реализованной героем древнегреческой мифологии Одиссеем. В операционную систему они обычно внедряются в результате целенаправленно проведенной операции, после чего сами становятся частью защищенной компьютерной системы и совершают действия, ради которых и были созданы.

Внедрение компьютерных вирусов по сути близко к применению программных закладок, отличие же заключается в том, что цель внедрения — модификация и уничтожение информации, хранящейся в компьютерных системах конкурентов.

Аппаратные закладки — это специальные микросхемы, выполняющие те же функции, что и программные закладки, либо радиозакладные устройства, аналогичные описанным в п. 1.3.1 и 1.5.2. Они могут перехватывать информацию, например, с клавиатуры или видеокарты, либо фиксировать аудиоинформацию (переговоры операторов), а затем передавать ее по радиоканалу в пункт приема. Известны в том числе и радиозакладки, которые активизируют компьютерные вирусы по команде, передаваемой по радиоканалу с пульта дистанционного управления.

Кроме того, перехват аудио- и видеоинформации может осуществляться с помощью технических средств, размещенных в том же помещении, что и компьютер (п. 1.3, 1.4).

Проблеме перехвата побочных электромагнитных излучений и наводок (ПЭМИН) в современной литературе уделяется большое внимание ввиду важности этого технического канала утечки информации. Здесь же мы только отметим, что наиболее сильные электромагнитные излучения образуются от сигналов с выхода видеокарты системного блока, для которых случайной антенной служит кабель, идущий к монитору. Для перехвата этой информации достаточно иметь приемное устройство, работающее в диапазоне частот 50... 500 МГц, специальный блок согласования и портативный компьютер типа Notebook. Дальность перехвата информации таким комплексом составляет 100...150 м.

Наиболее специфичным способом получения конфиденциальной информации с компьютерных систем является преодоление программных средств защиты и как его разновидность — преодоление систем парольной защиты. Рассмотрим их подробнее.

### 1.6.2. Преодоление программных средств защиты

В настоящее время известно огромное количество хакерских разработок, предназначенных для преодоления программных средств защиты. Они обладают различной эффективностью, но позволяют в той или иной степени решать задачи, ради которых созданы.

Одни из таких программ предназначены для перехвата сообщений и полномочий по доступу к ресурсам сети посредством незаконного подключения к каналу связи, другие — для преодоления системы защиты персонального компьютера или корпоративной сети другим зарегистрированным пользователем.

Перехват с незаконным подключением к каналу связи может осуществляться множеством способов, наиболее известными из которых являются:

- работа в сети в те промежутки времени, когда законный пользователь оставляет канал в активном режиме, отвлекаясь на решение других задач (вызов к начальнику, перекур и т. п.);
- работа параллельно зарегистрированному пользователю, но в те моменты, когда нет непосредственного обмена информацией, так называемый режим между строк (аналогичен предыдущему способу, но более сложен в реализации);
- работа по завершению сеанса зарегистрированным пользователем за счет перехвата сигнала об окончании работы.

Для преодоления систем защиты под видом зарегистрированного пользователя хакеры часто применяют следующие методы:

- перебор возможных паролей, которые часто бывают тривиальны и берутся из руководства по пользованию компьютером;
- поиск слабых мест (брешей), связанных с неудачным алгоритмом функционирования систем защиты или наличием программных ошибок;
- иногда брешь маскируется двумя-тремя дополнительными командами с целью создания так называемого люка, который открывается при необходимости (данный способ требует очень высокого профессионального уровня и готовится, как правило, на этапе проектирования системы защиты);
- использование программ, имитирующих аварийные сбои и анализирующих адекватность реакции системы.

Однако существует большое число программных продуктов, созданных совершенно для иных целей, но которые могут быть использованы для преодоления систем защиты, размещенных на жестких дисках. К ним, например, относятся уже упомянутые **Norton Utilities**, а также **Miced Utilities**, **PC Tools**, **PS Shell**, **Hard Disk Manager** и некоторые другие, которые в интерактивном или автоматическом режиме используют команды

считывания и записи секторов по абсолютным адресам на диске.
Также существуют разработки, которые позволяют создавать программное обеспечение, способное выполнять просмотр и отладку программных продуктов в режиме дисассемблера, а также просмотр и редактирование оперативной памяти персональной ЭВМ. К таким программам относятся трансляторы с языков низкого уровня (TASM и MASM), трансляторы с языков высокого уровня (**MSC, Turbo C, Turbo Pascal** и др.), программы-отладчики типа **The IBM Personal Computer Fulscreen Debug (FSD), Advanced Fulscreen Debug (AFD) и Turbo Debugger**, а также программы, работающие с оперативной памятью **(Debug, Peck Poke Resident),** и некоторые другие.

### 1.6.3. Преодоление парольной защиты

Один из наиболее распространенных способов разграничения доступа к ресурсам вычислительных систем — введение паролей. В целом это достаточно надежный способ защиты, однако необходимо представлять его возможности и основные способы преодоления, чтобы уберечь себя от неприятных последствий.
Так, в любом персональном компьютере можно условно выделить три вида паролей:
>• пароли, хранящиеся в CMOS-памяти;
>• пароли операционной системы;
>• пароли, по которым осуществляется аутентификация пользователей в специально установленной системе защиты.
Рассмотрим способы преодоления каждого вида в отдельности.

**Снятие паролей, хранящихся в CMOS-памяти**

CMOS — это аббревиатура английских слов complementary metal oxide semiconductor. То есть в качестве названия вида памяти взято просто наименование материала, из которого изготавливается соответствующая микросхема. В ней записывается вся необходимая информация для загрузки компьютера, в том числе и пароли. Еще -их называют «паролями BIOS» по названию микросхем, контролирующих операции ввода — вывода.
Доступ к установкам CMOS осуществляется нажатием во время теста памяти (при загрузке компьютера) одной из следующих комбинаций клавиш:
**Del;**
**Esc;**
**Ctrl + Alt + Enter;**
**Ctrl + Alt + Esc.**
При этом на экран выводится **меню установок CMOS**, среди которых присутствуют два раздела:
**SUPERVISOR PASSWORD** (пароль диспетчера);
**USER PASSWORD** (пароль пользователя).
Владелец первого пароля может осуществлять как загрузку операционной системы, так и изменение опций в меню «Установки BIOS»; человек, знакомый только со вторым паролем, может осуществлять загрузку операционной системы и только входить в меню «Установки BIOS» для изменения раздела «User Password».
Однако надежность такой парольной защиты является кажущейся. Существуют как минимум два довольно простых метода ее преодоления.
Первый основан на том, что CMOS-память не может работать без питания от батарейки, установленной внутри системного блока. Таким образом, если, отключив от сети компьютер и вскрыв системный блок, извлечь батарейку, то в памяти исчезнет информация о типе жестких дисков, числе и емкости флоппи-дисков, размере оперативной памяти и т. д., в том числе исчезнет информация и о хранящихся паролях. Положение батарейки CMOS может быть различным в разных компьютерах, но найти ее несложно по характерному внешнему виду: плоская маленькая в виде таблетки либо кассета из нескольких пальчиковых батареек.
После извлечения батарейку можно тут же поставить на место — память

очищена. Затем необходимо закрыть системный блок и включить компьютер. На этапе тестирования памяти (при загрузке) следует войти в меню «Установки BIOS» вышеуказанным способом и восстановить установки CMOS, естественно, за исключением паролей. К сожалению, последняя операция необходима, иначе в ходе загрузки система выдаст на экран следующее сообщение:

**INVALID SYSTEM SETTING — RUN SETUP**

(Неправильная системная установка — выполните установку).

Чтобы выполнить эту процедуру, надо либо заранее выяснить все необходимые сведения об установках, либо просто иметь определенные знания и опыт в данной области.

Второй способ в принципе повторяет первый и специально предусмотрен конструкторами на случай забывания пароля. Его применение даже описано в руководстве пользователя.

Так, например, на системной (материнской) плате компьютера Pentium установлена специальная перемычка **JP9** (рис. 1.6.1), предназначенная для очистки CMOS(СМ.Сноску 1). Нормальное положение перемычки, соответствует замыканию контактов 1—2 (табл. 1.6.1).

В том случае, если необходимо снять неизвестный или забытый пароль, то, предварительно отключив компьютер от сети и вскрыв системный блок, перемычка переставляется в положение 2—3. Затем включается компьютер, снова отключается и перемычка вновь возвращается в положение 1—2.

После завершения процедуры очистки CMOS-памяти необходимо осуществить настройку BIOS Setup («Установок BIOS») так же, как и в первом случае.

___

Сноска 1. Пример взят для платы TX 1 PHOENIX. На аналогичных платах других типов компьютеров оригинальный номер этой перемычки может быть другим. Он указан в руководстве по эксплуатации платы.

___

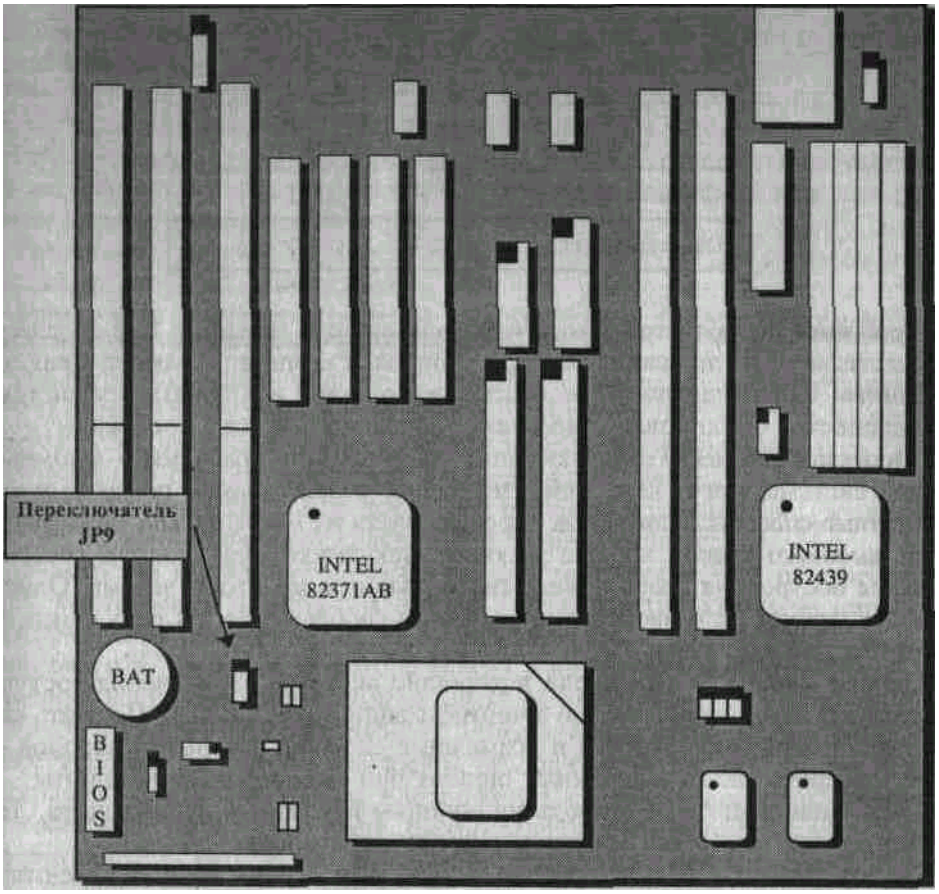



**Рис. 1.6.1. Расположение переключателя JP9 (очистки CMOS-памяти) на системной плате компьютера Pentium**

**Преодоление паролей операционной системы.** Разные операционные системы имеют разную стойкость к несанкционированному доступу.

Так, одной из наиболее защищенных операционных систем по праву считается Windows NT, обладающая уровнем зашиты **C2**, а Windows'95 (наиболее распространенная в настоящее время операционная система) из возможных средств защиты предлагает только введение пользовательских паролей и шифрование таблицы паролей. Однако, по большому счету, эти пароли вообще не могут рассматриваться как сколь-нибудь серьезное средство разграничения доступа. Дело в том, что их основное назначение — это обеспечение индивидуальной настройки рабочего стола для создания максимальных удобств пользователям при работе: зарегистрировался под своим паролем — получил свои настройки.

**Таблица 1.6.1. Значения положений JP9: перемычка сброса CMOS**

| Режим работы компьютера | Номера замкнутых контактов |
|---|---|
| Нормальный | 1-2 |
| Очистка CMOS | 2-3 |

Проблема заключается в том, что пользователи, которые имеют доступ к средствам редактирования реестра, например к опции **Password** (пароли) из **Control Panel** (панели управления), легко могут отключить эту систему безопасности, блокировав применение пользовательских профилей.

**Перехват паролей.** Реальную защиту информации, хранящейся в компьютерной системе, могут дать лишь специально разработанные программные и аппаратные способы защиты, так как преодолеть их могут **только специалисты** очень высокого класса, хорошо знающие атакуемую операционную систему, способы построения современных систем защиты и

методы взлома. Описывать эти методы не позволяют ни этические соображения, ни цель книги, ни объем настоящей главы.
Однако многие, в том числе и хорошие системы ограничения доступа, используют пароли как средство аутентификации пользователей. Показать слабые места парольной защиты и возможные способы раскрытия паролей — значит уберечь вас от возможных ошибок при выборе системы защиты.
Парольная защита — отнюдь не синоним понятию плохая защита. Тем не менее, она имеет как минимум две слабые стороны.
**Первая** связана с тем, что пароли, по которым осуществляется аутентификация пользователей, должны где-то храниться. Обычно это таблица паролей, входящая в состав программного обеспечения операционной системы или системы защиты. Следовательно, любой достаточно хорошо подготовленный пользователь тем или иным способом может проникнуть в соответствующий файл, скопировать или изменить его.
Именно благодаря данному обстоятельству выбираемая вами система защиты должна предусматривать кодирование таблицы паролей, что нивелирует ценность попытки проникновения в таблицу.
**Вторая** связана с возможностью тайного внедрения программной закладки в компьютерную систему, которая позволит злоумышленнику осуществлять несанкционированный доступ к информационным ресурсам. Перехватчики паролей — один из наиболее распространенных видов программных закладок. Они перехватывают пароли, применяемые для регистрации пользователей операционной системы, а также для определения их легальных полномочий и прав доступа к компьютерным ресурсам.
Перехватчики — отнюдь не новое явление. В свое время они успешно разрабатывались для OS/370, UNIX и DOS. Принцип действия у них достаточно традиционен и заключается в фиксации пароля на этапе регистрации пользователя. Далее пароль записывается в специальный файл, из которого он может быть легко извлечен. Различия между перехватчиками заключаются только в способах, которые применяются ими для получения пользовательских паролей.
Различают три типа перехватчиков паролей: имитаторы системы регистрации, фильтры и заместители.
Программы **имитаторы системы регистрации** достаточно легко реализуемы и функционируют по следующему алгоритму.
Имитатор первым реагирует на желание пользователя зарегистрироваться и предлагает ему ввести пароль. После того как пользователь идентифицирует себя (введет кодовую комбинацию), программная закладка скопирует пароль в специальный файл и далее инициирует выход из системы. В результате перед глазами пользователя появится еще одно, но уже настоящее регистрационное приглашение для входа в систему.
Обманутый пользователь, видя, что ему предлагают еще раз ввести пароль, естественно приходит к выводу, что допустил какую-то ошибку и повторяет всю процедуру ввода. Для того чтобы притупить бдительность пользователя, на экран монитора может выводиться соответствующее сообщение, например: «Неверный пароль! Попробуйте еще раз!»
Такой тип перехватчика паролей обладает одним очень существенным недостатком, а именно — сообщение об ошибке возникает при каждой регистрации, что не может не насторожить даже самого неискушенного пользователя. Более совершенный тип закладки-имитатора может сам сообщать системе пароль без вывода повторного приглашения. Выявить такую закладку уже можно только по косвенным признакам.
Принцип действия программ **фильтров** заключается в перехвате всей информации, вводимой с клавиатуры компьютера, и анализе ее (фильтрации) с целью выявления отношения к пользовательским паролям.
Известны несколько фильтров, созданных специально для различных версий операционной системы DOS, Windows 3.11 и Windows'95. По оценкам

специалистов, это один из наиболее легко реализуемых видов программных закладок-перехватчиков паролей. Дело в том, что в операционных системах Windows 3.11 и Windows'95 предусмотрен специальный программный механизм, с помощью которого решается ряд задач, связанных с получением доступа к клавиатурному вводу. Например, задача поддержки национальных раскладок клавиатур. Таким образом, любой русификатор — это фильтр, призванный перехватывать все данные, вводимые пользователем с клавиатуры. Небольшая доработка позволяет наделить этот фильтр дополнительной функцией — перехвата пароля. Задача облегчается еще и тем, что во многих учебных пособиях по Windows имеются исходные тексты программных русификаторов.

В ряде случаев проблема сводится лишь к способу внедрения видоизмененного текста русификатора вместе с подлинным. Если она успешно решена, то вся информация, вводимая с клавиатуры, будет проходить через фильтр и проверяться на принадлежность к паролям.

**Заместители** — программные модули, которые полностью или частично заменяют истинные, отвечающие в системе защиты за аутентификацию пользователей. Существенным достоинством заместителей является возможность работы в среде практически любой многопользовательской системы.

Недостаток — сложность создания и внедрения. По трудоемкости они так существенно опережают имитаторы и фильтры, что делает применение этого типа перехватчиков паролей вашими конкурентами практически маловероятным

### 1.6.4. Некоторые способы внедрения программных закладок и компьютерных вирусов

Созданием программной закладки или вируса еще не решается задача, поставленная при их написании. Вторая, не менее сложная, заключается во внедрении программного продукта. О важности и сложности этой последней задачи говорит тот факт, что ее решением в рамках информационной борьбы занимаются даже государственные структуры ряда стран. Такой «государственный» подход не оставляет сомнений в том, что самые новейшие достижения в области «имплантации» уже в скором времени станут достоянием промышленного шпионажа.

На сегодняшний день можно выделить три основные группы способов внедрения программных закладок и компьютерных вирусов:

- на этапе создания аппаратуры и программного обеспечения;
- через системы информационного обмена;
- силовым или ВЧ-навязыванием.

Наиболее просто ввести вирус **на этапе создания** элементов компьютерных систем. Ведь ни для кого не секрет, что современные программные продукты содержат примерно до полумиллиона строк, и никто лучше авторов-программистов их не знает, и поэтому эффективно проверить не может. В связи с этим создатели программного обеспечения являются потенциальными объектами для определенных служб и компаний. Однако более перспективным направлением, по сравнению с вербовкой программистов, эксперты считают инфицирование (модификацию) систем искусственного интеллекта, помогающих создавать это программное обеспечение.

Другим направлением внедрения является **использование систем информационного обмена.** Здесь существует два способа — непосредственное и косвенное подключение.

Непосредственное подключение (front-door coupling) бывает прямое и непрямое.

Прямое заключается в повторяющейся трансляции вирусного сигнала или программной закладки в период получения приемником конкурента предназначенной ему полезной информации. При этом можно рассчитывать,

что в какой-то момент времени, смешанный с основной информацией указанный программный продукт попадет в систему. Недостаток такого способа — необходимость знания используемых алгоритмов шифрования и ключей при передаче в канале закрытой информации.

В связи с последним обстоятельством более предпочтительным считается использование непрямого подключения. Проникновение в информационную систему в этом случае происходит в самом незащищенном месте, откуда вирус или программная закладка могут добраться до назначенного узла. Благодаря широкому внедрению глобальных сетей такие места всегда могут быть найдены.

Косвенное подключение (back-door) представляет из себя целый спектр способов: от воздействия на систему через элементы, непосредственно не служащие основному назначению (например, через цепи электропитания), до умышленной передачи конкуренту инфицированной техники или программных продуктов.

Перспективным направлением внедрения программных закладок или вирусов в информационные системы представляется и использованием методов **силового** или **ВЧ-навязывания**, аналогичных рассмотренным в п. 1.3.5.

Разработкой соответствующих средств, по сообщениям зарубежной печати, занимается целый ряд компаний, например. Defense Advanced Research Projects Agency (США), Toshiba (Япония) и др. Ожидается, что благодаря их усилиям уже через пять лет окажется возможным внедрять программные продукты именно таким способом.

В наиболее простом виде процесс ВЧ-навязывания закладок и вирусов выглядит примерно следующим образом. Мощное высокочастотное излучение, промодулированное информационным сигналом, облучает объект электронно-вычислительной техники. В цепях компьютера или линии связи наводятся соответствующие напряжения и токи, которые определенным образом детектируются на полупроводниковых элементах схемы вычислительного средства. В результате вирус или закладка оказываются внедренными в компьютер.

Далее, по заранее намеченной программе они осуществляют сбор, первичную обработку данных и передачу их в заданный адрес по сети, либо уничтожение или модификацию определенной информации.

Наиболее узким местом такого способа внедрения является подбор мощности, частоты, вида модуляции и других параметров зондирующего сигнала в каждом конкретном случае.

### 1.7. Угрозы реальные и мнимые

Материалы данного раздела несколько не вписываются в общую концепцию книги, однако позволят ответить на вопрос, который наиболее часто задают при различного рода контактах со специалистами по защите информации их потенциальные клиенты: «Насколько реально столкнуться в России с техническими средствами промышленного шпионажа?» На Западе такой вопрос со стороны бизнесмена будет воспринят как, мягко говоря, несколько наивный. В качестве иллюстрации того, как там ограждают себя от возможных неприятностей, связанных с утечкой информации по каналам технической разведки, приведем материал из газеты «Московский комсомолец» (от 12 апреля 2000 года). В Англии разразился очередной скандал, связанный с так называемыми газетными девочками — теми, что живут торговлей публикациями в прессе своих амурных приключений с различными знаменитостями. В данном случае скандал получился особенно громким: для «желтой прессы» роман официантки сразу с двумя всемирно знаменитыми футболистами — П. Гасконом и Р. Гуллитом — это убойная, почти историческая сенсация.

При этом отметим такую деталь: официантка в течение 8 месяцев тайно встречалась с Гуллитом раза два-три в недельку в его шикарном номере отеля. Перед встречами голландец с помощью электронного детектора

тщательно проверял стены на предмет «жучков». Возможно поэтому о секс-приключениях знаменитости не знала ни одна живая душа. Из этого примера видно, что в отличие от некоторых наших «профи» опасение технических средств негласного съема информации на Западе буквально в крови даже у людей, очень далеких от органов правопорядка.

И такое поведение вполне адекватно, поскольку преступления с использованием высоких технологий не менее опасны, чем проделки «отморозков» с автоматами. Недобросовестная конкурентная борьба или подрыв репутации — это такое же насилие над личностью, как удар топором по голове. Разорение крупных фирм влечет за собой крушение судеб многих людей. Кто-то из них никогда не оправится от удара и не найдет в себе силы начать с нуля, а кто-то даже покончит с собой. Компромат, подрывающий имидж, например, эстрадной звезды, на «раскрутку» которой потрачены миллионы, иногда очень жестко бьет не только по самолюбию, но и по карману. «Убойный» компромат, как правило, раз и навсегда ломает карьеру политика или госчиновника. Вместе с тем, следует признать, что Россия к технической войне с преступностью оказалась не готова. По данным прессы, Сергей Степашин, еще в бытность свою главой МВД, во время одного из международных саммитов, где обсуждались вопросы борьбы с международной преступностью, почувствовал себя в глубокой луже. Руководители правоохранительных органов стран «большой восьмерки» обсуждали меры противодействия в сфере высоких технологий. Нашим же по признанию самого Степашина сказать было нечего...

Поэтому, возвратившись домой, главный милиционер России в августе 1998 года сразу подписал приказ о создании специального управления «Р». Так появилось на свет одно из самых секретных подразделений МВД, задачей которого стала борьба с преступлениями в области высоких технологий. Результаты появились мгновенно: только за первые полгода своего существования новобранцы возбудили более 20 уголовных дел, а отдел по борьбе с незаконным оборотом специальных технических средств (СТС) изъял только радиотелефонов и приемников на сумму свыше 3 млн рублей, да еще прочей аппаратуры типа «жучков» и диктофонов — свыше 100 штук («МК» от 16 декабря 1999 года). Вместе с результатами появились весьма острые публикации в газетах, пошли сюжеты на телевидении, это сразу изменило ту благостную картину, что сложилась в воображении у подавляющего большинства граждан России по данной проблеме (вспомним знаменитое: «Секса у нас нет»).

Действительно, если подойти к проблеме промышленного шпионажа серьезно, то для того, чтобы данная отрасль деятельности получила на рынке услуг свою экономическую нишу, необходимо наличие следующих условий:

>• спроса на конфиденциальную информацию;

>• специалистов, способных удовлетворить этот спрос;

>• относительно доступного рынка спецтехники.

Что касается наличия спроса, то данный вопрос мы подробно рассмотрим в разделе 2.2, но думаем, что в условиях рыночных отношений вопрос звучит чисто риторически. Нет недостатка и в «свободных» специалистах по негласному съему информации. Но если на Западе люди, занимающиеся такого рода деятельностью, в достаточно большом количестве появились еще в начале 60-х годов, то мы столкнулись с подобной проблемой только в конце 80-х, когда государство перестало тотально контролировать сферу «хай технолоджи». А сейчас в России уже действуют не кустари-одиночки, а преступные группы, прекрасно оснащенные технически и готовые выполнить любой заказ с применением достаточно совершенного оборудования, ранее доступного только спецслужбам.

Для иллюстрации этого тезиса приведем несколько примеров. 18 мая 2000 года генерал А. Зданович в интервью программе ОРТ подробно рассказал о пресечении в городе Москве сотрудниками ФСБ деятельности Национального

фонда политических технологий. Данный с позволения сказать «фонд» занимался тайным сбором и продажей информации для проведения черных пиаровских акций. При обыске были изъяты многочисленные материалы, включая досье на ряд ведущих политиков, в частности данные об источниках финансировании Г. Явлинского и его партии «Яблоко». Через несколько дней в передаче «Человек и закон» была продолжена эта тема. При этом был раскрыт один из каналов, по которому информация такого рода поступала в «хранилища» фонда. Все оказалось просто — во дворе одного из элитных московских домов уже довольно долгое время без движения стояла черная иномарка. Но назвать ее беспризорной было нельзя: каждый вечер, изо дня в день, к ней подходил средних лет мужчина, открывал машину и на несколько минут скрывался в салоне. В один далеко не самый лучший для хозяина автомобиля вечер, он был при выходе из салона задержан сотрудниками ФСБ.

В машине был обнаружен панорамный приемник, с присоединенным к нему миниатюрным магнитофоном. Задержанный, оказавшийся отставным работником спецслужб, не стал запираться и немедленно признался в том, что производил замену кассеты в магнитофоне, на который записываются переговоры с домашнего телефона известного московского адвоката. Для обеспечения съема информации он установил в распределительную коробку телефонный «жучок». Показания подтвердились: с помощью детектора поля оперативники быстро нашли и изъяли весьма профессионально установленную радиозакладку. Все эти манипуляции были засняты на пленку и представлены телезрителям. Расследование показало, что «слухач» работал на вышеупомянутый фонд, который своей собственной спецтехники не имел, а за весьма солидную плату нанимал для выполнения разовых заданий специалистов — как правило, из числа бывших сотрудников спецслужб, ставших безработными.

Впрочем, «левым» заработком не брезгуют и некоторые действующие сотрудники весьма уважаемых ведомств. В городе Сыктывкаре (Республика Коми) завершились судебные слушания по беспрецедентному уголовному делу. Бывшему прапорщику одного из подразделений ФАПСИ — сотруднику Центра правительственной связи В. Покрушеву было предъявлено обвинение в незаконном прослушивании телефонных переговоров. Вот что пишет по этому поводу газета «Коммерсант» (№82 от 11 мая 2000 г.) «В октябре 1998 года прапорщик, как потом выяснило следствие, установил в шкафу с телефонными кабелями телефонный радиопередатчик. Его интересовали разговоры, которые вел по своему служебному телефону вице-президент республиканской федерации русского хоккея. Точкой для прослушивая Покрушев выбрал детский сад в полусотне метров от интересовавшего его здания, заявив работникам садика, что ловит опасного рецидивиста. «Жучок» в шкафу случайно обнаружили монтеры и сдали находку в ФСБ. Но чекисты интереса к прибору не проявили.

Следующая зафиксированная следствием вылазка бойца невидимого фронта пришлась на май 1999 года. К Покрушеву обратился частный предприниматель, друг которого подозревал свою жену в неверности. Прицепить «жучка» к проводу не составило никакого труда. Многодневное прослушивание подтвердило самые худшие опасения ревнивого супруга. Он даже решил «заказать» обидчика. Попытку убийства рубоповцы к счастью успели пресечь. Заказчик получил 4 года, а несостоявшийся киллер отделался условным наказанием.

Покрушев же был пойман только в августе 1999 года, когда сканировал переговоры с домашнего телефона генерального директора ОАО «Комитекс». Вычислил «жучка» начальник службы безопасности фирмы. Он нашел радиопередатчик в щите с телефонными проводами. Покрыл его поверхность спецсоставом, видимым лишь в ультрафиолетовых лучах, и после этого обратился в ФСБ. Поскольку информация, поступающая с такого мини-

передатчика, доступна лишь в радиусе 100 метров, схватить за руку охотника за компроматом не составило труда. Сотрудники ФСБ нашли следы спецсостава на ручке одной из дверей первого этажа этого же подъезда. Выяснили, что квартиру снимает их коллега из ФАПСИ и стали следить за Покрушевым. Взяли его на улице, а в арендуемой квартире помимо аппаратуры оперативники нашли множество кассет с перехваченной информацией как делового, так и интимного содержания. Хотя вина прапорщика была вполне доказана, отделался он легко — штрафом в 100 МРОТ (около 8500 руб.). Орудия «труда» — широкодиапазонный сканер, наушники, диктофон, комплект соединительных проводов и прочая аппаратура были конфискованы. Уволенный из ФАПСИ В. Покрушев по-прежнему трудится в системе связи — правда, теперь уже гражданской».

Нередки случаи, когда «шпион» сам ищет клиентов в активном режиме. В качестве примера приведем отрывок из статьи «Нашествие "клопов"», опубликованной в газете «Московский комсомолец» (от 16 декабря 1999 года). «— Как-то ко мне обратился «пряник» вполне интеллигентного вида, — рассказывает предприниматель из крупного российского города, занимающийся рекламой, — и предложил информацию о моих конкурентах: с какими фирмами ведут переговоры по установке щитов, на сколько «падают» в расценках при подписании договоров, сколько платят «черняком», а сколько — через банк, как много отстегивают чиновникам в городском управлении архитектуры за подписание проектов и предоставление выгодных мест, и кому именно... В общем, полный набор «компры» вплоть до записей телефонных переговоров. С этим я мог не только утопить конкурентов, но и перетащить на свою сторону их высоких покровителей. Жалко, не сошлись в цене. Парень был из Москвы и не представлял себе наши финансовые возможности. А напоследок кинул мне «подлянку». Сканировал номера моего домашнего и сотового телефона и дал объявление в газету, что по этому номеру продаются мангусты...».

Ну, а чтобы более четко обозначить масштабы проблемы, приведем еще несколько небольших выдержек из одной популярной московской газеты — «Коммерсант» (№ 91 от 24 мая 2000 года): «Вчера налоговая полиция обыскала 42 здания, принадлежащих АвтоВазу. По официальным данным, акция была проведена в рамках расследования уголовного дела... Кроме того, ФСНП изъяла в офисе спецтехнику съема информации и выявления подслушивающих устройств (похоже эти находки становятся фирменным знаком ФСНП)».

«Коммерсант» (№67 от 21 апреля 1999 года): «Прокуратура Приморского края изъяла в офисе крупной судоходной компании «Востоктрансфлот» прослушивающую аппаратуру. По версии губернатора Е. Наздратенко коммерсанты шпионили за краевой администрацией. Спецтехнику отправили на криминалистическую экспертизу...».

«Коммерсант» (№ 55 от 3 апреля 1999 года): «Сотрудники Мосгорпрокуратуры провели вчера обыск в офисе охранной фирмы «СБ Конус». Обыск проводился в рамках уголовного дела о незаконном вмешательстве в частную жизнь граждан. «Конус» якобы раздобыл и разместил в Интернете конфиденциальные данные о ряде известных политиков, артистов, бизнесменов и журналистов».

Ясно, что появление этих вопиющих фактов стало возможно только после того, как все вышеперечисленные злоумышленники смогли обзавестись соответствующей спецтехникой. Каким же образом она попадает в руки преступников? Вот как смотрит на этот вопрос газета «Московский комсомолец» (от 9 декабря 1999 года): «...Поскольку подобные «игрушки» подлежат обязательному лицензированию, то импортная аппаратура попадает на наш рынок контрабандой. Продекларированную как «бытовая техника» продукцию таможенники могут свободно пропустить в Россию. И дело тут не во взятках. Чтобы понять, что на самом деле представляет собой

«безобидный» приемник **AR** «мэйд ин Джапан», нужно быть специалистом высокого класса в области электроники. По словам Юрия Дудина, начальника отдела, занимающегося борьбой с незаконным оборотом специальных технических средств, продажей спецтехники из-под полы балуются и вполне легальные поставщики. Мол, отчего же не продать хорошим ребятам, у которых проблемы с конкурентами?

Подобные «игрушки» активно продаются на «Горбушке» и в Митине — ведь такую аппаратуру действительно можно использовать в качестве «мобильников» и радиоприемников. Тот же **AR** на рынке стоит сейчас порядка 1000 долларов. Несколько дороговато для простого любителя попсы. Радиотелефон с возможностью сканирования закрытых частот тянет как минимум на 400 долларов. Такую аппаратуру покупают люди, заинтересованные в чужих секретах. Поэтому оперативники отдела вместе с ОМОНом регулярно делают набеги на эти рынки, чтобы изъять из оборота шпионские штучки.

Поскольку иностранное оборудование — штука весьма дорогостоящая (один комплекс по сканированию переговоров абонентов сотовой связи производства Японии или Германии стоит более 10 000 $), к делу подключились наши отечественные умельцы. Тем более, что невостребованными оказались не только просто хорошие инженеры-электронщики, но и спецы, ранее работавшие в системе радиоразведки спецслужб. Недавно я стал свидетелем операции по ликвидации такого «кружка умелые руки». Оперативная группа управления «Р» вломилась в лабораторию НИИ с очень серьезным названием. В небольшой комнатке научного учреждения несколько головастых ребят наладили производство сканирующих устройств для расшифровки переговоров по сотовой связи и пейджинговых сообщений. По сути шпионской аппаратуры для богатеньких буратин с гипертрофированным любопытством по отношению к конкурирующим фирмам, а также для почтенных граждан, балующихся заказными убийствами, похищениями людей и шантажом.

Один из задержанных нехотя демонстрирует прибор. Он втыкает несколько штекеров, включает компьютер, и на мониторе плывут сообщения, адресованные одной из крупнейших московских пейджинговых компаний. На соседнем столе — недоделанный комплекс для сканирования переговоров сотовой связи с последующим выводом текста на компьютер.

— Схема разработана нами, — объясняет один из задержанных. — По каталогу мы выписываем необходимые детали, после чего делаем заказ одному из подмосковных радиозаводов. Мало ли сейчас оборонных предприятий, подрабатывающих всевозможными халтурами? Они нам собирают платы, естественно, не догадываясь, для чего прибор предназначен. А потом мы уже доводим прибор в этой мастерской, настраиваем и готовим с продаже.

Свою рекламу «электронные жуки» размещали в Интернете. Кто знает, сколько убийств и вымогательств совершено после того, как преступники с помощью этого оборудования сумели снять информацию о своих жертвах? Статья 138 УК, предусматривающая наказание за незаконное изготовление и использование спецтехники, а также за нарушение тайны переписки и телефонных переговоров, подразумевает лишь штраф или условное наказание. Законодатели не учли, что использование спецтехники всегда влечет за собой или подготовку преступления, или попытку его скрыть. В тех же Штатах давно это поняли, поэтому за подобные художества там можно запросто получить 20 лет лишения свободы».

Кроме организованных групп успешно действуют и умельцы-одиночки. Вот что писала об одном из таких «феноменов» газета «Санкт-Петербургские ведомости» (№95 от 25 мая 2000 года): «Несанкционированное прослушивание, столь распространенное сейчас в сфере бизнеса и криминала, — это целая индустрия разнообразных технических средств и

способов их установки. Другая отдельная область — это распознавание «жучков» и противодействие им. И вот представьте, все это разом сведено на нет одним человеком. Ибо его оборудование для прослушивания — это простой домашний компьютер, подключаемый через модем к самой обычной телефонной розетке, но позволяющее без особого труда прослушать любой телефонный разговор на пространстве бывшего СССР и большинства стран мира. А установить факт прослушивания и определить, где находится «ухо» совершенно невозможно.

Для организованных преступных группировок изобретение питерского гения — просто клад. Бандиты «слушают» конкурентов и партнеров по бизнесу, неверных жен и подозреваемых в измене собственных «братков». Без сбора предварительной информации о потенциальной жертве не обходится ни одно серьезное заказное убийство. К примеру, после покушения на заместителя начальника РУБОПа Н. Акулова на его лестничной площадке были обнаружены следы нелегальной «прослушки». И потому давать в руки криминальному миру столь мощное техническое средство позволить было нельзя.

Бизнес уже был налажен неплохо — к примеру, недавно один гражданин США купил сразу аж 30 устройств. Удалось выяснить, что «товар», который представляет собой модифицированный модем и дискету с программой, стоит 5000 долларов. Опытнейших сыщиков даже гениальному хакеру, разумеется, провести не удалось. Задержание состоялось на пороге охранной фирмы, где работал подставной «покупатель». Перед этим хакер продемонстрировал все возможности своего детища, получил меченые деньги, и тут же оказался в крепких руках оперативников 5-го отдела РУБОП. Привезенный на Чайковского, 30, он организовал показательный сеанс прослушивания. Сел за компьютер, поиграл клавишами, и из недр «электронного ящика» раздался родной до боли голос начальника отдела, проводившего контрольный разговор в соседнем кабинете. Вызванный эксперт по безопасности Петербургской телефонной сети от изумления буквально онемел. Анализ изобретения показал: чтобы поставить барьер этому «спруту», нужно поменять полностью (!) все оборудование сети. Кстати, несколько лет назад хакер предлагал свои услуги руководству службы безопасности «Петерстара». Разумеется, ему тогда показали на дверь — кто же допустит в святая святых такого безумца.

Сейчас специалисты в сути изобретения разобрались досконально и вынуждены согласиться, что невозможное стало возможным. Но как с этим бороться, сегодня никто не знает, а несколько десятков экземпляров чудо-техники гуляет на воле. В отношении умельца возбуждено уголовное дело по статье 138 УК. Статья слабенькая — даже по самой суровой 3-й части, где как раз говорится о производстве и сбыте спецтехники для негласного получения информации, она предполагает максимум три года лишения свободы. Увы, законодатель не учел, что нарушение тайны важно не само по себе, а может стать первым шагом для совершения самых тяжких и кровавых преступлений».

Из приведенного материала видно, что угроза пострадать от применения спецтехники негласного съема информации преступными элементами в России более чем реальна для любого человека, независимо от его положения. Вместе с тем, подавляющее большинство законопослушных граждан боятся совсем другого, а при появлении даже признаков «прослушки» все валят на происки спецслужб. Особенно не повезло в этом отношении телефону. Телефонная связь у нас всегда была окружена легендами. Давно, когда советская интеллигенция вела по своим кухням полночные беседы, одной из их главных тем было то, что вездесущие органы слушают не только наши телефонные разговоры, но даже через молчащий телефон слышат то, о чем говорят в домах. В нынешние либеральные времена у нашего государства тайн от народа, похоже, нет. Без пугающего грифа «секретно» выпущен приказ министра связи В. Булгака № 135 от 8 ноября 1995 года, где

сказано: «Система технических средств по обеспечению оперативно-розыскных мероприятий должна устанавливаться на отечественных и импортных электронных телефонных станциях всех телефонных сетей: общего пользования, ведомственных и выделенных сетей, независимо от их форм собственности».

А поскольку техника идет вперед, то вскоре возник новый приказ (№ 9 от 31 января 1996 года): «Технические средства по обеспечению оперативно-розыскных мероприятий должны устанавливаться на сетях подвижной связи (сети радиотелефонной связи общего пользования, сети персонального радиовызова и выделенные сети радиосвязи) независимо от форм собственности. Система должна обеспечивать: контроль исходящих и входящих вызовов (местных внутризонных, междугородних и международных) к/от абонентов данной станции, а также контроль вызовов к заранее заданным номерам. При предоставлении абоненту услуги по переадресации вызовов на другого абонента должен контролироваться как номер абонента, заказывающего эту услугу, так и номер, на который заказана переадресация... Контролируемым абонентам должна присваиваться одна из следующих категорий контроля: а) полный контроль; б) статистический контроль. При полном контроле на пункт управления (ПУ) передаются в реальном масштабе времени информация о фазах установления соединения, данные о контролируемых вызовах, а также осуществляется съем и трансляция на ПУ информации, передаваемой в разговорном тракте контролируемого абонента».

После даже беглого ознакомления с данным документом, самые элементарные соображения здравого смысла, типа «от добра добра не ищут», напрочь исключат спецслужбы из перечня организаций, которые по «компетентному» мнению многих доморощенных «акул пера» устанавливают «жучки» в линиях связи, или безвылазно сидят на каждой АТС. Эта самая популярная у обывателей угроза явно относится к категории мнимых. Поэтому, при обнаружении в своих средствах коммуникации «под слушки», можно смело обращаться в милицию. Поскольку, чтобы иметь доступ «к заранее заданному номеру», спецслужбам необходимо только получить у судьи соответствующую санкцию, а это при наличии законных оснований сделать гораздо проще, и главное безопасней, чем проникать в офис или копаться в хитросплетениях телефонной сети.

Дополнительной опасности подвергается информация владельцев компьютеров, которые подключены к различного вида сетям. Основная угроза при этом исходит от хакеров и компьютерных вирусов.

Хакерством в той или иной степени балуются многие представители технической молодежи, считая это своего рода популярной тусовкой. Подавляющая часть этого рода-племени через какое-то время забывает о своих занятиях, другие же, наоборот, начинают заниматься им профессионально, зарабатывая весьма неплохие деньги. Очень интересное исследование этой проблемы провела солидная, совершенно не склонная к дешевым сенсациям газета «Санкт-Петербургские ведомости», опубликовав большую статью «Питерские хакеры: кто они?» (№ 110 от 16 июня 2000 года). Позволим себе процитировать из нее небольшой отрывок: «В Петербурге сегодня обитает примерно три-четыре десятка хакерских групп, а количество кланов, занимающихся «профдеятельностью» за деньги, составляет пять— восемь. Как и везде, хакерские группы делятся на три вида. К первому типу относится специально подобранная, централизованно руководимая группа специалистов, нанятая фирмой или государством для определенных задач. Информация по ним крайне закрытая.

Ко второму типу можно отнести самообразовавшуюся среду, где есть несколько умных людей, которые имеют свое помещение, «крышу» и постоянный контингент заказчиков. В Питере, насколько мне известно, две таких «бригады». Первая сидит на базе института, состоит из 18 человек,

занимается отслеживанием компьютерного и софтового рынка. Их объявления (завуалированные под предложения ремонта и настройки) можно встретить в рекламных газетах. Вторая уже три года как переросла в фирму, торгующую «железом», но по старой памяти они осуществляют и спецзаказы. Клиентам в поставленные машины зашивается «жучок» в виде фирменного вируса, который может воздействовать на компьютер без ведома его нового хозяина.

Третий тип — это стихийно образовавшийся клан, не имеющий централизованного управления, но тем не менее состоящий из разбирающихся в своем деле людей. Принцип существования — постоянный подбор новых кадров и массовость, позволяющая защитить своих членов от чьих-либо «наездов». Как вы понимаете, таких кланов наибольшее количество. Интернетом они интересуются только как полигоном для тренировки. Поле деятельности отличается многообразием, но ломают чаще всего системы типа «клиент-банк» у ничего не подозревающих главбухов, путем зависания на телефонной линии».

Ну, а чтобы читатели смогли оценить реальные возможности некоторых хакеров, процитируем еще одно место из вышеуказанной статьи: «Третьего фигуранта нашего списка зовут Метео. Свою известность сей джентльмен получил благодаря взломам различных коммерческих программ. Примечательна его эпопея с одной нашей фирмой, которая занимается производством электронных ключей. Как только у фирмы выходила новая версия, Метео тут же ее взламывал. Что самое смешное, продолжалась эта эпопея почти целый год».

Таким образом, можно смело сказать, что проблема хакеров, а значит и наличие опасности взлома компьютерной сети, у нас в России никак не может быть отнесена к мнимой угрозе. Дополнительной иллюстрацией к этому очевидному факту является следующая любопытная информация. В августе 1998 года в Санкт-Петербурге был арестован М. Орлов, директор 000 «Орлов и К» за торговлю компакт-дисками с базами данных Петербургской телефонной сети. В апреле 1999 года Выборгский районный суд признал обвиняемого виновным по статье 272 УК (неправомерный доступ к компьютерной информации) и назначил ему наказание — 1 год 3 месяца лишения свободы в колонии общего режима. Этот приговор стал прецедентом для Петербурга. Впервые в городе было доведено до конца уголовное дело по статье, наказывающей за компьютерное пиратство. А вот знаменитого питерского хакера Левина (№ 1 по классификации газет) арестовали в Великобритании, а судили в США.

Не меньшим ореолом таинственности, чем хакеры, окружены компьютерные вирусы. Интересно, что у неспециалистов по этому вопросу существует два прямо противоположных мнения. Одни считают, что вирусы большого вреда принести не могут, а представляют собой что-то вроде насморка. Другие, наоборот, приводят «ужасающие истории» о полном перехвате управления машиной, вплоть до убийств через компьютер его хозяина. Конечно последнее является явным преувеличением, но эпидемии таких вирусов, как Melissa, «Чернобыль», LoveLetter, показывают, что первые тоже неправы, и ни один из пользователей не застрахован от разрушительного действия вирусов. Чтобы окончательно развеять оба эти заблуждения, приведем информацию специалистов о некоторых наиболее опасных представителях данного семейства.

Вот что пишет на эту тему газета «Коммерсант» (№ 72 от 28 апреля 1999 года): «26 апреля телефоны в российских антивирусных центрах раскалились с самого утра. Поступило около полутысячи звонков и более 100 электронных писем из 20 с лишним городов России. Пользователи жаловались, что компьютеры отказываются работать и перезагружаться. Многие полагали, что у них вышел из строя блок питания, но дело было не в нем:

сработал вирус «Чернобыль», запущенный в оборот год назад неизвестными тайваньскими «вирусописателями». На прошлой неделе специалисты предупреждали о его предстоящей активизации, но не все восприняли предупреждения всерьез. Причем это единственный вирус, который имеет серьезные деструктивные функции. Сначала он пытается испортить содержимое микросхемы Flash BIOS, которое компьютер считывает при запуске, а затем стирает данные на жестком диске. Если вирусу удалось испортить BIOS, владельцу ПК придется менять эту микросхему или перепрограммировать ее на специальном оборудовании. Впрочем на некоторых типах ноутбуков придется менять всю начинку — легче купить новый. Что касается пропавших данных, то в большинстве случаев восстановить их практически невозможно.

Больше всего пострадали страны с высоким уровнем компьютерного пиратства, — ведь вирус живет в семи из каждых десяти пиратских компакт-дисков. В Южной Корее вышло из строя 300 000 компьютеров (ущерб более 250 млн $). Легче всех отделались США — всего несколько сотен поврежденных ПК. Лучшей рекламы антивирусные фирмы и придумать не могли: недостатка в клиентах они сейчас не испытывают. Горячие денечки наступили и у фирм, занимающихся восстановлением данных на диске. Стоит это более 200 $. Впрочем те, кто в результате «вирусной атаки» лишился дипломной работы, диссертации или базы данных, за ценой не постоят».

Газета «Коммерсант» привела материалы о еще одном вирусе (№ 24 **от** 25 мая 2000 года): «В начале мая резко возросло число объяснений в любви. Признавались секретарши и клерки, парламентарии и министры, инженеры и менеджеры. Признавались, сами того не ведая, адресуя свои послания тем, кого сами не знали. Эпидемия этой всесокрушающей любви вспыхнула 4 мая, когда неизвестный хакер изготовил и разослал по Интернету новый компьютерный вирус-червь, получивший название LoveLetter. А дальше «червь» начал, рассылать сам себя веерным способом— он отправлял свои копии по всем адресам электронной почты из адресной книги.

Активизированный вирус не только рассылал копии, но и внедрялся в операционную систему зараженного компьютера. В каталоге Windows он создавал файлы со своими копиями, причем таким образом, что при каждом перезапуске он вновь активизировался. Кроме того, вирус скачивал из Интернета и устанавливал в систему так называемого троянского коня, которому при очередном перезапуске передавалось управление. «Троянец» выуживал из компьютера всю конфиденциальную информацию (IP-адреса, сетевой login, пароли и т. д.) и отсылал ее по заранее указанному адресу. А потом «червь» уничтожал файлы на всех доступных дисках... По некоторым оценкам, убытки от LoveLetter достигают 10 млрд $. Трудности борьбы с «червями» заключаются в том, что стандартные антивирусные средства способны отловить опасного гостя только после того, как он проник в систему и поразил ее».

Из приведенного материала видно, что вирусы — мощный дополнительный канал, через который может происходить как утечка, так и потеря (разрушение) информации. Положение, однако, вовсе не безнадежное. Отказываться от использования компьютеров в Интернете, как это советуют некоторые «специалисты», нет причин. Просто нужно искать способы решения проблемы вирусов, и, поверьте, такие решения уже существуют. До сих пор использовались лишь антивирусные программы, называемые сканерами, но они «брали» только известного врага. При появлении новых разновидностей требовалось определенное время, чтобы антивирусные компании смогли получить образец нового вируса, создать противоядие и разослать его пользователям. Тем временем вирус «гуляет на свободе».

Новое поколение антивирусных программ, лидером в разработке которых является Россия, получило название блокираторы или «песочницы». Дело в том, что вирус производит некоторую последовательность действий.

Например, незаметно отключает встроенную антивирусную программу пакета Microsoft. Это значит, что если некая программа будет блокировать такие действия, то пользователь будет застрахован от бед. Другое направление — «ревизор изменений». Вирусы, внедряясь в другие файлы, производят в них изменения. Вот эти изменения отслеживают «ревизоры» — и сообщают пользователю. Главное преимущество таких программ, по мнению одного из ведущих «вирусологов» России Евгения Касперского, состоит в том, что даже если «ревизор» обнаружит следы уже внедренного вируса, он предоставляет практически 100% возможность восстановить содержимое зараженных файлов.

Когда мы подбирали выше изложенный материал, то, конечно же, не ставили задачу напугать обывателя, а хотели дать своего рода информацию к размышлению. Наша главная цель — показать, что возможность стать жертвой той или иной разновидности промышленных шпионов в современной России из экзотики стала, увы, суровой реальностью. Настолько суровой, что не слишком богатое МВД было вынуждено создать новое управление, на которое возложена борьба с такого рода преступлениями. А теперь перейдем ко второй части книги, где рассмотрим основные методы борьбы с этими опасными деяниями. Однако сразу хотим предупредить, что взятое по отдельности каждое из средств противодействия, которые будут нами вскоре описаны, малоэффективно, а для создания по-настоящему надежной защиты все они должны быть элементами полноценной системы безопасности.

# Глава вторая

## ЗАЩИТА ИНФОРМАЦИИ ОТ ПРОМЫШЛЕННОГО ШПИОНАЖА

## 2.1. Нормативно-правовая база защиты информации

### 2.1.1. Роль и место правового обеспечения

Разработка методов и средств защиты от промышленного шпионажа является важной составной частью общегосударственного процесса построения системы защиты информации. Значимость этого процесса определяется прежде всего глобальностью тех преобразований, которые происходят в настоящее время в политической и экономической жизни России.

Дело в том, что та система защиты информационных ресурсов, которая существовала в стране до 1991 года, в силу объективных причин оказалась разрушенной. Построение же новой системы в нынешних условиях — задача сложная, кроме того она усугубляется целым рядом факторов, основными из которых являются:

>• информационная и технологическая экспансия США и других развитых стран, осуществляющих глобальный мониторинг мировых политических, экономических, военных, экологических и других процессов, распространяющих информацию в целях получения односторонних преимуществ;

>• нарушение информационных связей вследствие образования независимых государств на территории бывшего СССР;

>• стремление России к более тесному сотрудничеству с зарубежными странами в процессе проведения реформ на основе максимальной открытости сторон;

>• расширяющаяся кооперация с зарубежными странами в области развития информационной инфраструктуры России;
>• низкая общая правовая и информационная культура в российском обществе;
>• переход России на рыночные отношения в экономике, появление множества отечественных и зарубежных коммерческих структур — производителей и потребителей информации, средств информатизации и защиты информации, включение информационной продукции в систему товарных отношений;
>• критическое состояние отечественных отраслей промышленности, производящих средства информатизации и защиты информации;
>• недостаточная нормативно-правовая база в сфере информационных отношений, в том числе в области обеспечения информационной безопасности;
>• слабое регулирование государством процессов функционирования и развития рынка средств информатизации, информационных продуктов и услуг в России;
>• широкое использование в сфере государственного управления и кредитно-финансовой сфере незащищенных от утечки информации импортных технических и программных средств для хранения, обработки и передачи информации;
>• рост объемов информации, передаваемой по открытым каналам связи, в том числе по сетям передачи данных и межмашинного обмена;
>• обострение криминогенной обстановки, рост числа компьютерных преступлений, особенно в кредитно-финансовой сфере.

Построение четко работающей системы защиты информации, призванной, в том числе, решать и задачи противодействия промышленному шпионажу, возможно только на основе эффективного сочетания правовых, программно-технических и организационных мер. Интересно, что, по данным некоторых зарубежных исследований, удельный вес каждого из перечисленных компонентов соответственно составляет:

>• правовые методы — 60 %;
>• программно-технические — 30 %;
>• организационные методы — 10 %.

Из приведенных цифр наглядно видно, что правовые методы занимают лидирующее место по своей значимости, и именно поэтому правовое обеспечение рассматривается как приоритетное направление в политике обеспечения информационной безопасности Российской Федерации. Правовое обеспечение включает в себя:

а) нормотворческую деятельность по созданию законодательства, регулирующего общественные отношения в области информационной безопасности;

б) исполнительную и правоприменительную деятельность по исполнению законодательства в области информации, информатизации и защиты информации органами государственной власти и управления, организациями (юридическими лицами), гражданами.

Нормотворческая деятельность в области обеспечения информационной безопасности предусматривает:

>• оценку состояния действующего законодательства и разработку программы его совершенствования;
>• создание организационно-правовых механизмов обеспечения информационной безопасности;
>• формирование правового статуса всех субъектов в системе информационной безопасности, пользователей информационных и телекоммуникационных систем и определение их ответственности за обеспечение информационной безопасности;

>• разработку организационно-правового механизма сбора и анализа статистических данных о воздействии угроз информационной безопасности и их последствиях с учетом всех видов (категорий) информации;

>• разработку законодательных и других нормативных актов, регулирующих порядок ликвидации последствий воздействий угроз, восстановления нарушенного права и ресурсов, реализации компенсационных мер;

Исполнительная и правоприменительная деятельность предусматривает:

>• разработку процедур применения законодательства и нормативных актов к субъектам, совершившим преступления и проступки при работе с закрытой информацией и нарушившим регламент информационных взаимодействий, а также совершившим правонарушения с использованием незащищенных средств информатизации;

>• разработку составов правонарушений с учетом специфики уголовной, гражданской, административной, дисциплинарной ответственности.

Вся деятельность по правовому обеспечению информационной безопасности должна строиться на основе трех фундаментальных положений права — соблюдение законности, обеспечение баланса интересов отдельных субъектов и государства, неотвратимость наказания.

Соблюдение законности предполагает наличие законов и иных нормативных установлений, их применение и исполнение субъектами права в области информационной безопасности.

Обеспечение баланса интересов граждан, других субъектов информационных отношений и государства предусматривает приоритет государственных интересов как общих интересов всех субъектов. Ориентация на свободы, права и интересы граждан не принижает роль государства в обеспечении национальной безопасности в целом и в области информационной безопасности в частности.

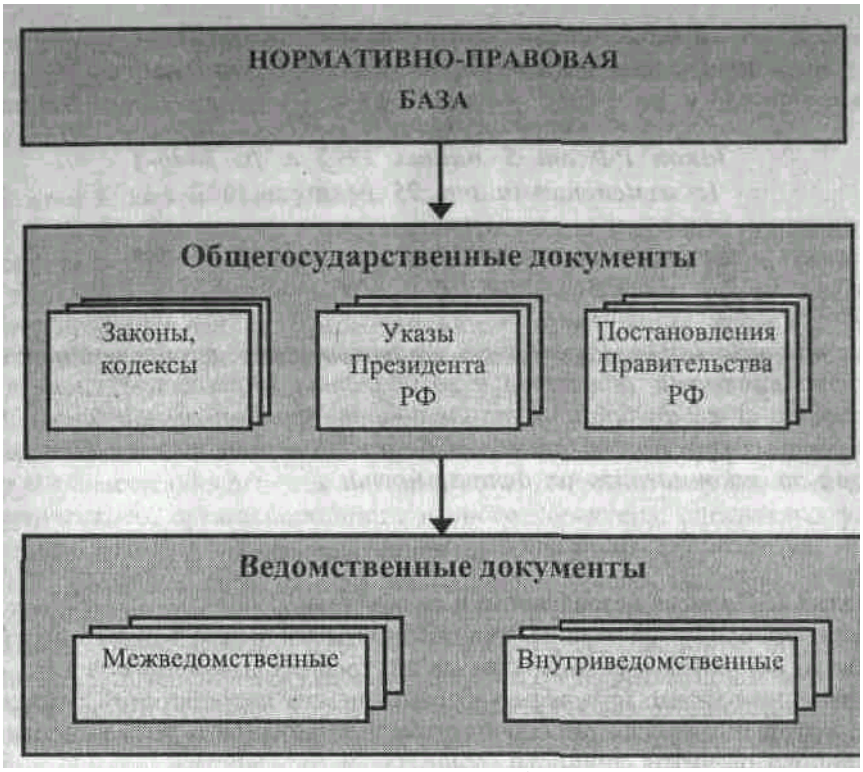



**Рис. 2.1.1. Нормативно-правовая база защиты информации**

Неотвратимость наказания выполняет роль важнейшего профилактического инструмента в решении вопросов правового обеспечения.

Весь комплекс документов, обеспечивающих нормативно-правовую базу,

формируется на двух основных иерархических уровнях (рис. 2.1.1): государственном и ведомственном.
На государственном уровне формируются законы, кодексы, указы Президента и Постановления Правительства Российской Федерации, направленные на построение системы информационной безопасности и регламентирующие информационные отношения в обществе в целом.
На втором уровне формируется комплекс межведомственных и внутриведомственных нормативно-методических документов, обеспечивающих функционирование системы информационной безопасности.
Строго говоря, существует еще один — третий — уровень, призванный обеспечить взаимоотношения между юридическими и физическими лицами по вопросам сохранения коммерческой (негосударственной) тайны. Однако формируемые на этом уровне документы относятся уже не к нормативно-правовому обеспечению, а к организации защиты информации.

**2.1.2. Общегосударственные документы по обеспечению информационной безопасности «О БЕЗОПАСНОСТИ» Закон РФ от 5 марта 1992 г. № 2446-1 (с изменениями от 25 декабря 1992 г.)**

Введен в действие Постановлением ВС РФ от 5 марта 1992 г. № 2446/1-1.
Настоящий Закон закрепляет правовые основы обеспечения безопасности личности, общества и государства, определяет систему безопасности и ее функции, устанавливает порядок организации и финансирования органов обеспечения безопасности, а также контроля и надзора за законностью их деятельности.

**Раздел I. Общие положения**

**Статья 1. Понятие безопасности и ее объекты**

Безопасность — состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.
Жизненно важные интересы — совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства.
К основным объектам безопасности относятся: личность — ее права и свободы; общество — его материальные и духовные ценности; государство — его конституционный строй, суверенитет и территориальная целостность.

**Статья 2. Субъекты обеспечения безопасности**

Основным субъектом обеспечения безопасности является государство, осуществляющее функции в этой области через органы законодательной, исполнительной и судебной властей.
Государство в соответствии с действующим законодательством обеспечивает безопасность каждого гражданина на территории Российской Федерации. Гражданам Российской Федерации, находящимся за ее пределами, государством гарантируется защита и покровительство.
Граждане, общественные и иные организации и объединения являются субъектами безопасности, обладают правами и обязанностями по участию в обеспечении безопасности в соответствии с законодательством Российской Федерации, законодательством республик в составе Российской Федерации, нормативными актами органов государственной власти и управления краев, областей, автономной области и автономных округов, принятыми в пределах их компетенции в данной сфере. Государство обеспечивает правовую и социальную защиту гражданам, общественным и иным организациям и объединениям, оказывающим содействие в обеспечении безопасности в соответствии с законом.

**Статья 3. Угроза безопасности**

Угроза безопасности — совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства.
Реальная и потенциальная угроза объектам безопасности, исходящая от внутренних и внешних источников опасности, определяет содержание деятельности по обеспечению внутренней и внешней безопасности.

**Статья 4. Обеспечение безопасности**

Безопасность достигается проведением единой государственной политики в области обеспечения безопасности, системой мер экономического, политического, организационного и иного характера, адекватных угрозам жизненно важным интересам личности, общества и государства.

Для создания и поддержания необходимого уровня защищенности объектов безопасности в Российской Федерации разрабатывается система правовых норм, регулирующих отношения в сфере безопасности, определяются основные направления деятельности органов государственной власти и управления в данной области, формируются или преобразуются органы обеспечения безопасности и механизм контроля и надзора за их деятельностью.

Для непосредственного выполнения функций по обеспечению безопасности личности, общества и государства в системе исполнительной власти в соответствии с законом образуются государственные органы обеспечения безопасности.

**Статья 5. Принципы обеспечения безопасности**

Основными принципами обеспечения безопасности являются:

>• законность;

>• соблюдение баланса жизненно важных интересов личности, общества и государства;

>• взаимная ответственность личности, общества и государства по обеспечению безопасности;

>• интеграция с международными системами безопасности.

**Статья 6. Законодательные основы обеспечения безопасности**

Законодательные основы обеспечения безопасности составляют Конституция РСФСР, настоящий Закон, законы и другие нормативные акты Российской Федерации, регулирующие отношения в области безопасности;

конституции, законы, иные нормативные акты республик в составе Российской Федерации и нормативные акты органов государственной власти и управления краев, областей, автономной области и автономных округов, принятые в пределах их компетенции в данной сфере; международные договоры и соглашения, заключенные или признанные Российской Федерацией.

**Статья 7. Соблюдение прав и свобод граждан при обеспечении безопасности**

При обеспечении безопасности не допускается ограничение прав и свобод граждан, за исключением случаев, прямо предусмотренных законом.

Граждане, общественные и иные организации и объединения имеют право получать разъяснения по поводу ограничения их прав и свобод от органов, обеспечивающих безопасность. По их требованию такие разъяснения даются в письменной форме в установленные законодательством сроки.

Должностные лица, превысившие свои полномочия в процессе деятельности по обеспечению безопасности, несут ответственность в соответствии с законодательством.

**Раздел II. Система безопасности Российской Федерации**

**Статья 8. Основные элементы системы безопасности**

Систему безопасности образуют органы законодательной, исполнительной и судебной властей, государственные, общественные и иные организации и объединения, граждане, принимающие участие в обеспечении безопасности в соответствии с законом, а также законодательство, регламент" тирующее отношения в сфере безопасности.

Создание органов обеспечения безопасности, не установленных законом Российской Федерации, не допускается.

**Статья 9. Основные функции системы безопасности**

Основными функциями системы безопасности являются:

>• выявление и прогнозирование внутренних и внешних угроз жизненно

важным интересам объектов безопасности, осуществление комплекса оперативных и долговременных мер по их предупреждению и нейтрализации;

>• создание и поддержание в готовности сил и средств обеспечения безопасности;

>• управление силами и средствами обеспечения безопасности в повседневных условиях и при чрезвычайных ситуациях;

>• осуществление системы мер по восстановлению нормального функционирования объектов безопасности в регионах, пострадавших в результате возникновения чрезвычайной ситуации;

>• участие в мероприятиях по обеспечению безопасности за пределами Российской Федерации в соответствии с международными договорами и соглашениями, заключенными или признанными Российской Федерацией.

**Статья 10. Разграничение полномочий органов власти в системе безопасности**

Обеспечение безопасности личности, общества и государства осуществляется на основе разграничения полномочий органов законодательной, исполнительной и судебной властей в данной сфере.

Указом Президента РФ от 24 декабря 1993 г. No 2288 часть вторая статьи 10 настоящего Закона признана недействующей.

Верховный Совет Российской Федерации:

>• определяет приоритеты в защите жизненно важных интересов объектов безопасности;

>• разрабатывает систему правового регулирования отношений в сфере безопасности;

>• устанавливает порядок организации и деятельности органов обеспечения безопасности;

>• осуществляет контроль за кадровой политикой государственных органов обеспечения безопасности;

>• не реже одного раза в год заслушивает доклад Президента Российской Федерации об обеспечении безопасности Российской Федерации;

>• определяет бюджетные ассигнования на финансирование органов обеспечения безопасности и федеральных программ в сфере безопасности;

>• ратифицирует и денонсирует международные договоры и соглашения Российской Федерации по вопросам обеспечения безопасности.

Органы исполнительной власти:

>• обеспечивают исполнение законов и иных нормативных актов, регламентирующих отношения в сфере безопасности;

>• организуют разработку и реализацию государственных программ обеспечения безопасности;

>• осуществляют систему мероприятий по обеспечению безопасности личности, общества и государства в пределах своей компетенции;

>• в соответствии с законом формируют, реорганизуют и ликвидируют государственные органы обеспечения безопасности.

Судебные органы:

>• обеспечивают защиту конституционного строя в Российской Федерации, руководствуясь Конституцией РСФСР и законами Российской Федерации, конституциями и законами республик в составе Российской Федерации;

>• осуществляют правосудие по делам о преступлениях, посягающих на безопасность личности, общества и государства;

>• обеспечивают судебную защиту граждан, общественных и иных организаций и объединений, чьи права были нарушены в связи с деятельностью по обеспечению безопасности.

**Статья 11. Руководство государственными органами обеспечения безопасности**

Общее руководство государственными органами обеспечения безопасности

осуществляет Президент Российской Федерации.
Президент Российской Федерации:
>• возглавляет Совет безопасности Российской Федерации;
(Указом Президента РФ от 24 декабря 1993 г. No 2288 абзацы третий и шестой части второй статьи 11 настоящего Закона признаны недействующими.)
>• совместно с Верховным Советом Российской Федерации определяет стратегию обеспечения внутренней и внешней безопасности;
>• контролирует и координирует деятельность государственных органов обеспечения безопасности;
>• в пределах определенной законом компетенции принимает оперативные решения по обеспечению безопасности;
>• не реже одного раза в год представляет Верховному Совету Российской Федерации доклад об обеспечении безопасности Российской Федерации.
Совет Министров Российской Федерации (Правительство Российской Федерации):
>• в пределах определенной законом компетенции обеспечивает руководство государственными органами обеспечения безопасности Российской Федерации;
>• организует и контролирует разработку и реализацию мероприятий по обеспечению безопасности министерствами и государственными комитетами Российской Федерации, другими подведомственными ему органами Российской Федерации, республик в составе Российской Федерации, краев, областей, автономной области, автономных округов.
Министерства и государственные комитеты Российской Федерации:
>• в пределах своей компетенции, на основе действующего законодательства, в соответствии с решениями Президента Российской Федерации и постановлениями Правительства Российской Федерации обеспечивают реализацию федеральных программ защиты жизненно важных интересов объектов безопасности;
>• на основании настоящего Закона в пределах своей компетенции разрабатывают внутриведомственные инструкции (положения) по обеспечению безопасности и представляют их на рассмотрение Совета безопасности.

**Статья 12. Силы и средства обеспечения безопасности**

Силы и средства обеспечения безопасности создаются и развиваются в Российской Федерации в соответствии с решениями Верховного Совета Российской Федерации, указами Президента Российской Федерации, краткосрочными и долгосрочными федеральными программами обеспечения безопасности.
Силы обеспечения безопасности включают в себя: Вооруженные Силы, федеральные органы безопасности, органы внутренних дел, внешней разведки, обеспечения безопасности органов законодательной, исполнительной, судебной властей и их высших должностных лиц, налоговой службы;
службы ликвидации последствий чрезвычайных ситуаций, формирования - гражданской обороны; пограничные войска, внутренние войска; органы, обеспечивающие безопасное ведение работ в промышленности, энергетике, на транспорте и в сельском хозяйстве; службы обеспечения безопасности средств связи и информации, таможни, природоохранительные органы, органы охраны здоровья населения и другие государственные органы обеспечения безопасности, действующие на основании законодательства.
Службы Министерства безопасности Российской Федерации, Министерства внутренних дел Российской Федерации, иных органов исполнительной власти, использующие в своей деятельности специальные силы и средства, действуют только в пределах своей компетенции и в соответствии с* законодательством.

Руководители органов обеспечения безопасности в соответствии с законодательством несут ответственность за нарушение установленного порядка их деятельности.

**Раздел III. Совет безопасности Российской Федерации**

**Статья 13. Статус Совета безопасности Российской Федерации**

Совет безопасности Российской Федерации является конституционным органом, осуществляющим подготовку решений Президента Российской Федерации в области обеспечения безопасности.

Совет безопасности Российской Федерации рассматривает вопросы внутренней и внешней политики Российской Федерации в области обеспечения безопасности, стратегические проблемы государственной, экономической, общественной, оборонной, информационной, экологической и иных видов безопасности, охраны здоровья населения, прогнозирования, предотвращения чрезвычайных ситуаций и преодоления их последствий, обеспечения стабильности и правопорядка и ответствен перед Верховным Советом Российской Федерации за состояние защищенности жизненно важных интересов личности, общества и государства от внешних и внутренних угроз.

**Статья 14. Состав Совета безопасности Российской Федерации и порядок его формирования**

Совет безопасности Российской Федерации формируется на основании Конституции РСФСР, Закона РСФСР «О Президенте РСФСР» и настоящего Закона.

**Указом Президента РФ от 24 декабря 1993 г. Ns 2288 Закон РСФСР «О Президенте РСФСР» признан недействующим.**

В состав Совета безопасности Российской Федерации входят: председатель, секретарь, постоянные члены и члены Совета безопасности.

Председателем Совета безопасности является по должности Президент Российской Федерации.

Состав Совета Безопасности РФ утвержден Указом Президента РФ от 31 июля 1996 г. No 1121.

Указом Президента РФ от 24 декабря 1993 г. Ns 2288 части четвертая — шестая статьи 14 настоящего Закона признаны недействующими

В число постоянных членов Совета безопасности Российской Федерации входят по должности: вице-президент Российской Федерации, Первый заместитель Председателя Верховного Совета Российской Федерации, Председатель Совета Министров Российской Федерации (Председатель Правительства Российской Федерации).

Секретарь Совета безопасности входит в число постоянных членов Совета безопасности, назначается Президентом Российской Федерации и утверждается в должности Верховным Советом Российской Федерации.

Членами Совета безопасности могут являться руководители федеральных министерств и ведомств: экономики и финансов, иностранных дел, юстиции, обороны, безопасности, внутренних дел, экологии и природных ресурсов, здравоохранения, Службы внешней разведки, а также иные должностные лица, назначенные Президентом Российской Федерации с согласия Верховного Совета Российской Федерации.

Законом РФ от 25 декабря 1992 г. No 4235-1 статья 14 настоящего Закона дополнена частью седьмой. Части седьмая и восьмая считаются соответственно частями восьмой и девятой.

В заседаниях Совета безопасности принимает участие Председатель Верховного Совета Российской Федерации или по его поручению заместитель Председателя.

В зависимости от содержания рассматриваемого вопроса Совет безопасности Российской Федерации может привлекать к участию в заседаниях на правах консультантов и других лиц.

При рассмотрении вопросов обеспечения безопасности на территориях

республик в составе Российской Федерации, краев, областей, автономной области и автономных округов для участия в работе Совета безопасности привлекаются их полномочные представители, а также председатель Государственного комитета Российской Федерации по национальной политике.

**Статья 15. Основные задачи Совета безопасности Российской Федерации**

Основными задачами Совета безопасности Российской Федерации являются:

>• определение жизненно важных интересов личности, общества и государства и выявление внутренних и внешних угроз объектам безопасности;

>• разработка основных направлений стратегии обеспечения безопасности Российской Федерации и организация подготовки федеральных программ ее обеспечения;

>• подготовка рекомендаций Президенту Российской Федерации для принятия решений по вопросам внутренней и внешней политики в области обеспечения безопасности личности, общества и государства;

>• подготовка оперативных решений по предотвращению чрезвычайных ситуаций, которые могут повлечь существенные социально-политические, экономические, военные, экологические и иные последствия, и по организации их ликвидации;

>• подготовка предложений Президенту Российской Федерации о введении, продлении или отмене чрезвычайного положения;

>• разработка предложений по координации деятельности органов исполнительной власти в процессе реализации принятых решений в области обеспечения безопасности и оценка их эффективности;

>• совершенствование системы обеспечения безопасности путем разработки предложений по реформированию существующих либо созданию новых органов, обеспечивающих безопасность личности, общества и государства.

**Статья 16. Порядок принятия решений Советом безопасности Российской Федерации**

Заседания Совета безопасности Российской Федерации проводятся не реже одного раза в месяц. В случае необходимости могут проводиться внеочередные заседания Совета.

Постоянные члены Совета безопасности Российской Федерации обладают равными правами при принятии решений. Члены Совета безопасности принимают участие в его работе с правом совещательного голоса.

Решения Совета безопасности Российской Федерации принимаются на его заседании постоянными членами Совета безопасности простым большинством голосов от их общего количества и вступают в силу после утверждения председателем Совета безопасности.

Решения Совета безопасности по вопросам обеспечения безопасности оформляются указами Президента Российской Федерации.

**Статья 17. Межведомственные комиссии Совета безопасности Российской Федерации**

Совет безопасности Российской Федерации в соответствии с основными задачами его деятельности образует постоянные межведомственные комиссии, которые могут создаваться на функциональной или региональной основе.

В случае необходимости выработки предложений по предотвращению чрезвычайных ситуаций и ликвидации их последствий, отдельным проблемам обеспечения стабильности и правопорядка в обществе и государстве, защите конституционного строя, суверенитета и территориальной целостности Российской Федерации Советом безопасности Российской Федерации могут создаваться временные межведомственные комиссии.

Порядок формирования постоянных и временных межведомственных комиссий регламентируется Положением о Совете безопасности Российской Федерации,

утверждаемым Президентом Российской Федерации по согласованию с Верховным Советом Российской Федерации.

По решению Совета безопасности Российской Федерации постоянные и временные межведомственные комиссии могут возглавляться членами Совета безопасности, а также руководителями соответствующих министерств и ведомств Российской Федерации, их заместителями либо лицами, уполномоченными на то Президентом Российской Федерации.

**Статья 18. Аппарат Совета безопасности Российской Федерации**

Организационно-техническое и информационное обеспечение деятельности Совета безопасности Российской Федерации осуществляет его аппарат, возглавляемый секретарем Совета безопасности Российской Федерации,

Структура и штатное расписание аппарата Совета безопасности Российской Федерации, а также положения о его подразделениях утверждаются председателем Совета безопасности.

См. Положение об аппарате Совета безопасности Российской Федерации, утвержденное Указом Президента РФ от 1 августа 1996 г. № 1128.

**Статья 19. Основные задачи межведомственных комиссий и аппарата Совета безопасности Российской Федерации**

На межведомственные комиссии и аппарат Совета безопасности Российской Федерации возлагаются:

>• оценка внутренних и внешних угроз жизненно важным интересам объектов безопасности, выявление источников опасности;

>• подготовка научно обоснованных прогнозов изменения внутренних и внешних условий и факторов, влияющих на состояние безопасности Российской Федерации;

>• разработка и координация федеральных программ по обеспечению безопасности Российской Федерации и оценка их эффективности;

>• накопление, анализ и обработка информации о функционировании системы обеспечения безопасности Российской Федерации, выработка рекомендаций по ее совершенствованию;

>• информирование Совета безопасности Российской Федерации о ходе исполнения его решений;

>• организация научных исследований в области обеспечения безопасности;

>• подготовка проектов решений Совета безопасности Российской Федерации, а также проектов указов Президента Российской Федерации по вопросам безопасности;

>• подготовка материалов для доклада Президента Российской Федерации Верховному Совету Российской Федерации об обеспечении безопасности Российской Федерации.

**Раздел IV. Финансирование деятельности по обеспечению безопасности**

**Статья 20. Финансирование деятельности по обеспечению безопасности**

Финансирование деятельности по обеспечению безопасности в зависимости от содержания и масштабов программ, характера чрезвычайных ситуаций и их последствий осуществляется за счет средств республиканского бюджета Российской Федерации, бюджетов республик в составе Российской Федерации, краев и областей, автономной области, автономных округов, городов Москвы и Санкт-Петербурга, а также внебюджетных средств.

**Раздел V. Контроль и надзор за деятельностью по обеспечению безопасности**

**Статья 21. Контроль за деятельностью по обеспечению безопасности**

Указом Президента РФ от 24 декабря 1993 г. NQ 2288 часть первая статьи 21 настоящего Закона признана недействующей.

Контроль за деятельностью по обеспечению безопасности осуществляет Верховный Совет Российской Федерации через Совет Республики и Совет Национальностей Верховного Совета Российской Федерации, соответствующие постоянные комиссии палат и комитеты Верховного Совета Российской

Федерации в соответствии с действующим законодательством.
Органы государственной власти и управления Российской Федерации в пределах своей компетенции осуществляют контроль за деятельностью министерств и ведомств, предприятий, учреждений и организаций по обеспечению безопасности.
Общественные и иные объединения и организации, граждане Российской Федерации имеют право на получение ими в соответствии с действующим законодательством информации о деятельности органов обеспечения безопасности.

**Статья 22. Надзор за законностью деятельности органов обеспечения безопасности**

Надзор за законностью деятельности органов обеспечения безопасности осуществляет Генеральный прокурор Российской Федерации и подчиненные ему прокуроры.

**Москва, Дом Советов России**
**5 марта 1992 г. № 2446-1**
**Президент Российской Федерации Б. Ельцин**

**«ОБ ИНФОРМАЦИИ, ИНФОРМАТИЗАЦИИ И ЗАЩИТЕ ИНФОРМАЦИИ»**

**Федеральный закон от 20 февраля 1995 г. № 24-ФЗ Принят Государственной Думой 25 января 1995 г.**

**Глава 1. Общие положения**

**Статья 1. Сфера действия настоящего Федерального закона**

1. Настоящий Федеральный закон регулирует отношения, возникающие при:

>• формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации;

>• создании и использовании информационных технологий и средств их обеспечения;

>• защите информации, прав субъектов, участвующих в информационных процессах и информатизации.

2. Настоящий Федеральный закон не затрагивает отношений, регулируемых Законом Российской Федерации «Об авторском праве и смежных правах».

**Статья 2. Термины, используемые в настоящем Федеральном законе, их определения**

В настоящем Федеральном законе используются следующие понятия:

>• информация — сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

>• информатизация — организационный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов;

>• документированная информация (документ) — зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;

>• информационные процессы — процессы сбора, обработки, накопления, хранения, поиска и распространения информации;

>• информационная система — организационно упорядоченная совокупность документов (массивов документов и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы;

>• информационные ресурсы — отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных

системах);
>• информация о гражданах (персональные данные) — сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность;
>• конфиденциальная информация — документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации;
>• средства обеспечения автоматизированных информационных систем и их технологий — программные, технические, лингвистические, правовые, организационные средства (программы для электронных вычислительных машин; средства вычислительной техники и связи; словари, тезаурусы и классификаторы; инструкции и методики; положения, уставы; должностные инструкции; схемы и их описания, другая эксплуатационная и сопроводительная документация), используемые или создаваемые при проектировании информационных систем и обеспечивающие их эксплуатацию;
>• собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения — субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения указанными объектами;
>• владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения — субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах, установленных законом;
>• пользователь (потребитель) информации — субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

**Статья 3. Обязанности государства в сфере формирования информационных ресурсов и информатизации**

1. Государственная политика в сфере формирования информационных ресурсов и информатизации направлена на создание условий для эффективного и качественного информационного обеспечения решения стратегических и оперативных задач социального и экономического развития Российской Федерации.
2. Основными направлениями государственной политики в сфере информатизации являются:

**(Об основах государственной политики в сфере информатизации см. Указ Президента РФ от 20 января 1994 г. № 170.)**

>• обеспечение условий для развития и защиты всех форм собственности на информационные ресурсы;
>• формирование и защита государственных информационных ресурсов;
>• создание и развитие федеральных и региональных информационных систем и сетей, обеспечение их совместимости и взаимодействия в едином информационном пространстве Российской Федерации;
>• создание условий для качественного и эффективного информационного обеспечения граждан, органов государственной власти, органов местного самоуправления, организаций и общественных объединений на основе государственных информационных ресурсов;
>• обеспечение национальной безопасности в сфере информатизации, а также обеспечение реализации прав граждан, организаций в условиях информатизации;
>• содействие формированию рынка информационных ресурсов, услуг, информационных систем, технологий, средств их обеспечения;
>• формирование и осуществление единой научно-технической и промышленной политики в сфере информатизации с учетом современного мирового уровня развития информационных технологий;
>• поддержка проектов и программ информатизации;
>• создание и совершенствование системы привлечения инвестиций и

механизма стимулирования разработки и реализации проектов информатизации;

**>•** развитие законодательства в сфере информационных процессов, информатизации и защиты информации.

## Глава 2. Информационные ресурсы

**Статья 4. Основы правового режима информационных ресурсов**

1. Информационные ресурсы являются объектами отношений физических, юридических лиц, государства, составляют информационные ресурсы России и защищаются законом наряду с другими ресурсами.

2. Правовой режим информационных ресурсов определяется нормами, устанавливающими:

**>•** порядок документирования информации;

**>•** право собственности на отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах;

**>•** категорию информации по уровню доступа к ней;

**>•** порядок правовой защиты информации.

**Статья 5. Документирование информации**

1. Документирование информации является обязательным условием включения информации в информационные ресурсы. Документирование информации осуществляется в порядке, устанавливаемом органами государственной власти, ответственными за организацию делопроизводства, стандартизацию документов и их массивов, безопасность Российской Федерации.

2. Документ, полученный из автоматизированной информационной системы, приобретает юридическую силу после его подписания должностным лицом в порядке, установленном законодательством Российской Федерации.
3. Юридическая сила документа, хранимого, обрабатываемого и передаваемого с помощью автоматизированных информационных и телекоммуникационных систем, может подтверждаться электронной цифровой подписью.
Юридическая сила электронной цифровой подписи признается при наличии в автоматизированной информационной системе программно-технических средств, обеспечивающих идентификацию подписи, и соблюдении установленного режима их использования.
4. Право удостоверять идентичность электронной цифровой подписи осуществляется на основании лицензии. Порядок выдачи лицензий определяется законодательством Российской Федерации.

**Статья 6. Информационные ресурсы как элемент состава имущества и объект права собственности**

1. Информационные ресурсы могут быть и негосударственными и как элемент состава имущества находятся в собственности граждан, органов государственной власти, органов местного самоуправления, организаций и общественных объединений. Отношения по поводу права собственности на информационные ресурсы регулируются гражданским законодательством Российской Федерации.
2. Физические и юридические лица являются собственниками тех документов, массивов документов, которые созданы за счет их средств, приобретены ими на законных основаниях, получены в порядке дарения или наследования.
3. Российская Федерация и субъекты Российской Федерации являются собственниками информационных ресурсов, создаваемых, приобретаемых, накапливаемых за счет средств федерального бюджета, бюджетов субъектов Российской Федерации, а также полученных путем иных установленных законом способов.
Государство имеет право выкупа документированной информации у физических и юридических лиц в случае отнесения этой информации к государственной тайне.
Собственник информационных ресурсов, содержащих сведения, отнесенные к государственной тайне, вправе распоряжаться этой собственностью только с разрешения соответствующих органов государственной власти.
4. Субъекты, представляющие в обязательном порядке документированную информацию в органы государственной власти и организации не утрачивают своих прав на эти документы и на использование информации, содержащейся в них. Документированная информация, представляемая в обязательном порядке в органы государственной власти и организации юридическими лицами независимо о их организационно-правовой формы и форм собственности, а также гражданами на основании статьи 8 настоящего Федерального закона,
формирует информационные ресурсы, находящиеся в совместном **владении** государства и субъектов, представляющих эту информацию.
5. Информационные ресурсы, являющиеся собственностью **организаций**, включаются в состав их имущества в соответствии с гражданским законодательством Российской Федерации.
Информационные ресурсы, являющиеся собственностью государства, находятся в ведении органов государственной власти и организаций в соответствии с их компетенцией, подлежат учету и защите в составе государственного имущества.
6. Информационные ресурсы могут быть товаром, за исключением случаев, предусмотренных законодательством Российской Федерации.
См. Положение о порядке учета архивных документов при приватизации

государственного и муниципального имущества, утвержденное распоряжением Госкомимущества РФ от 22 октября 1996 г. NQ 1131-р, приказом Росархива от 6 ноября 1996 г. No 54.

1. Собственник информационных ресурсов пользуется всеми правами, предусмотренными законодательством Российской Федерации, в том числе он имеет право:

>• назначить лицо, осуществляющее хозяйственное ведение информационными ресурсами или оперативное управление ими;

>• устанавливать в пределах своей компетенции режим и правила обработки, защиты информационных ресурсов и доступа к ним;

•>• определять условия распоряжения документами при их копировании и распространении.

8. Право собственности на средства обработки информации не создает права собственности на информационные ресурсы, принадлежащие другим собственникам. Документы, обрабатываемые в порядке предоставления услуг или при совместном использовании этих средств обработки, принадлежат их владельцу. Принадлежность и режим производной продукции, создаваемой в этом случае, регулируются договором.

**Статья 7. Государственные информационные ресурсы**

1. Государственные информационные ресурсы Российской Федерации формируются в соответствии со сферами ведения как:

>• федеральные информационные ресурсы;

>• информационные ресурсы, находящиеся в совместном ведении Российской Федерации и субъектов Российской Федерации (далее — информационные ресурсы совместного ведения);

>• информационные ресурсы субъектов Российской Федерации.

2. Формирование государственных информационных ресурсов в соответствии с пунктом 1 статьи 8 настоящего Федерального закона осуществляется гражданами, органами государственной власти, органами местного самоуправления, организациями и общественными объединениями.

Федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации формируют государственные информационные ресурсы, находящиеся в их ведении, и обеспечивают их использование в соответствии с установленной компетенцией.

3. Деятельность органов государственной власти и организаций по формированию федеральных информационных ресурсов, информационных ресурсов совместного ведения, информационных ресурсов субъектов Российской Федерации финансируется из федерального бюджета и бюджетов субъектов Российской Федерации по статье расходов «Информатика» («Информационное обеспечение»).

4. Организации, которые специализируются на формировании федеральных информационных ресурсов и (или) информационных ресурсов совместного ведения на основе договора, обязаны получить лицензию на этот вид деятельности в органах государственной власти. Порядок лицензирования определяется законодательством Российской Федерации.

**Статья 8. Обязательное представление документированной информации для формирования государственных информационных ресурсов**

1. Граждане, органы государственной власти, органы местного самоуправления, организации и общественные объединения обязаны представлять документированную информацию органам и организациям, ответственным за формирование и использование государственных информационных ресурсов.

Перечни представляемой в обязательном порядке документированной информации и перечни органов и организаций, ответственных за сбор и обработку федеральных информационных ресурсов, утверждает Правительство Российской Федерации.

2. Порядок и условия обязательного представления документированной

информации доводятся до сведения граждан и организаций.
Порядок обязательного представления (получения) информации, отнесенной к государственной тайне, и конфиденциальной информации устанавливается и осуществляется в соответствии с законодательством об этих категориях информации.
3. При регистрации юридических лиц регистрационные органы обеспечивают их перечнями представляемых в обязательном порядке документов и адресами их представления. Перечень представляемой в обязательном порядке документированной информации прилагается к уставу каждого юридического лица (положению о нем).
Необеспечение регистрационными органами регистрируемых юридических лиц перечнем представляемых в обязательном порядке документов с адресами их представления не является основанием для отказа в регистрации. Должностные лица регистрационных органов, виновные в необеспечении регистрируемых юридических лиц перечнями представляемых в обязательном порядке документов с адресами их представления привлекаются к дисциплинарной ответственности вплоть до снятия с должности.
4. Документы, принадлежащие физическим и юридическим лицам, могут включаться по желанию собственника в состав государственных информационных ресурсов по правилам, установленным для включения документов в соответствующие информационные системы.

**Статья 9. Отнесение информационных ресурсов к общероссийскому национальному достоянию**

1. Отдельные объекты федеральных информационных ресурсов могут быть объявлены общероссийским национальным достоянием.
2. Отнесение конкретных объектов федеральных информационных ресурсов к общероссийскому национальному достоянию и определение их правового режима устанавливаются федеральным законом.

**Статья 10. Информационные ресурсы по категориям доступа**

1. Государственные информационные ресурсы Российской Федерации являются открытыми и общедоступными. Исключение составляет документированная информация, отнесенная законом к категории ограниченного доступа.
О степенях секретности сведений см.: Закон РФ от 21 июля 1993 г. Ns 5485-1 «О государственной тайне», постановление Правительства РФ от 4 сентября 1995 г. № 870.
2. Документированная информация с ограниченным доступом по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную.
3. Запрещено относить к информации с ограниченным доступом:
>• законодательные и другие нормативные акты, устанавливающие правовой статус органов государственной власти, органов местного самоуправления, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;
**>•** документы, содержащие информацию о чрезвычайных ситуациях, экологическую, метеорологическую, демографическую, санитарно-эпидемиологическую и другую информацию, необходимую для обеспечения безопасного функционирования населенных пунктов, производственных объектов, безопасности граждан и населения в целом;
**>•** документы, содержащие информацию о деятельности органов государственной власти и органов местного самоуправления, об использовании бюджетных средств и других государственных и местных ресурсов, о состоянии экономики и потребностях населения, за исключением отнесенных к государственной тайне;
>• документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах органов государственной власти, органов местного самоуправления, общественных объединений, организаций, представляющие общественный интерес или необходимые для реализации

прав, свобод и обязанностей граждан.
4. Отнесение информации к государственной тайне осуществляется в соответствии с Законом Российской Федерации «О государственной тайне».
5. Отнесение информации к конфиденциальной осуществляется в порядке, установленном законодательством Российской Федерации, за исключением случаев, предусмотренных статьей 11 настоящего Федерального закона.

**Статья 11. Информация о гражданах (персональные данные)**

1. Перечни персональных данных, включаемых в состав федеральных информационных ресурсов, информационных ресурсов совместного ведения, информационных ресурсов субъектов Российской Федерации, информационных ресурсов органов местного самоуправления, а также получаемых и собираемых негосударственными организациями, должны быть закреплены на уровне федерального закона. Персональные данные относятся к категории конфиденциальной информации.
Согласно Федеральному закону от 15 ноября 1997 г. No 143-ФЗ сведения, ставшие известными работнику органа записи актов гражданского состояния в связи с государственной регистрацией акта гражданского состояния, являются персональными данными.
О сборе, хранении, использовании и распространении информации о частной жизни см. Конституцию РФ от 12 декабря 1993 г.
См. Временный перечень сведений, составляющих конфиденциальную информацию в Пенсионном фонде Российской Федерации, утвержденный постановлением Правления ПФР от 30 августа 1996 г. NQ 123.
Перечень сведений конфиденциального характера утвержден Указом Президента РФ от 6 марта 1997 г. No 188.
Не допускаются сбор, хранение, использование и распространение информации о частной жизни, а равно информации, нарушающей личную тайну, семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений физического лица без его согласия, кроме как на основании судебного решения.
2. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.
3. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.
4. Подлежит обязательному лицензированию деятельность негосударственных организаций и частных лиц, связанная с обработкой и предоставлением пользователям персональных данных. Порядок лицензирования определяется законодательством Российской Федерации.
5. Неправомерность деятельности органов государственной власти и организаций по сбору персональных данных может быть установлена в судебном порядке по требованию субъектов, действующих на основании статей 14 и 15 настоящего Федерального закона и законодательства о персональных данных.

## Глава 3. Пользование информационными ресурсами

**Статья 12. Реализация права на доступ к информации из информационных ресурсов**

1. Пользователи — граждане, органы государственной власти, органы местного самоуправления, организации и общественные объединения — обладают равными правами на доступ к государственным информационным ресурсам и не обязаны обосновывать перед владельцами этих ресурсов необходимость получения запрашиваемой ими информации. Исключение составляет информация с ограниченным доступом.

Доступ физических и юридических лиц к государственным информационным ресурсам является основой осуществления общественного контроля за деятельностью органов государственной власти, органов местного самоуправления, общественных, политических и иных организаций, а также за состоянием экономики, экологии и других сфер общественной жизни.

2. Владельцы информационных ресурсов обеспечивают пользователей (потребителей) информацией из информационных ресурсов на основе законодательства, уставов указанных органов и организаций, положений о них, а также договоров на услуги по информационному обеспечению.

См. Положение об информационных услугах в области гидрометеорологии и мониторинга загрязнения окружающей природной среды, утвержденное постановлением Правительства РФ от 15 ноября 1997 г. No 1425.

Информация, полученная на законных основаниях из государственных информационных ресурсов гражданами и организациями, может быть использована ими для создания производной информации в целях ее коммерческого распространения с обязательной ссылкой на источник информации.

Источником прибыли в этом случае является результат вложенных труда и средств при создании производной информации, но не исходная информация, полученная из государственных ресурсов.

3. Порядок получения пользователем информации (указание места, времени, ответственных должностных лиц, необходимых процедур) определяет собственник или владелец информационных ресурсов с соблюдением требований, установленных настоящим Федеральным законом.

Перечни информации и услуг по информационному обеспечению, сведения о порядке и условиях доступа к информационным ресурсам владельцы информационных ресурсов и информационных систем предоставляют пользователям бесплатно.

4. Органы государственной власти и организации, ответственные за формирование и использование информационных ресурсов, обеспечивают условия для оперативного и полного предоставления пользователю документированной информации в соответствии с обязанностями, установленными уставами (положениями) этих органов и организаций.

5. Порядок накопления и обработки документированной информации с ограниченным доступом, правила ее защиты и порядок доступа к ней определяются органами государственной власти, ответственными за определенные вид и массивы информации, в соответствии с их компетенцией либо непосредственно ее собственником в соответствии с законодательством.

**Статья 13. Гарантии предоставления информации**

1. Органы государственной власти и органы местного самоуправления создают доступные для каждого информационные ресурсы по вопросам деятельности этих органов и подведомственных им организаций, а также в пределах своей компетенции осуществляют массовое информационное обеспечение пользователей по вопросам прав, свобод и обязанностей граждан, их безопасности и другим вопросам, представляющим общественный интерес.

2. Отказ в доступе к информационным ресурсам, предусмотренным в пункте 1 настоящей статьи, может быть обжалован в суд.

3. Комитет при Президенте Российской Федерации по политике информатизации организует регистрацию всех информационных ресурсов, информационных систем и публикацию сведений о них для обеспечения права граждан на доступ к информации.
О государственном учете и регистрации баз и банков данных см. постановление Правительства РФ от 28 февраля 1996 г. No 226.
4. Перечень информационных услуг, предоставляемых пользователям из государственных информационных ресурсов бесплатно или за плату, не возмещающую в полном размере расходы на услуги, устанавливает Правительство Российской Федерации.
Расходы на указанные услуги компенсируются из средств федерального бюджета и бюджетов субъектов Российской Федерации.

**Статья 14. Доступ граждан и организаций к информации о них**

1. Граждане и организации имеют право на доступ к документированной информации о них, на уточнение этой информации в целях обеспечения ее полноты и достоверности, имеют право знать, кто и в каких целях использует или использовал эту информацию. Ограничение доступа граждан и организаций к информации о них допустимо лишь на основаниях, предусмотренных федеральными законами.
2. Владелец документированной информации о гражданах обязан предоставить информацию бесплатно по требованию тех лиц, которых она касается. Ограничения возможны лишь в случаях, предусмотренных законодательством Российской Федерации.
3. Субъекты, представляющие информацию о себе для комплектования информационных ресурсов на основании статей 7 и 8 настоящего Федерального закона, имеют право бесплатно пользоваться этой информацией.
4. Отказ владельца информационных ресурсов субъекту в доступе к информации о нем может быть обжалован в судебном порядке.

**Статья 15. Обязанности и ответственность владельца информационных ресурсов**

1. Владелец информационных ресурсов обязан обеспечить соблюдение режима обработки и правил предоставления информации пользователю, установленных законодательством Российской Федерации или собственником этих информационных ресурсов, в соответствии с законодательством.
2. Владелец информационных ресурсов несет юридическую ответственность за нарушение правил работы с информацией в порядке, предусмотренном законодательством Российской Федерации.

**Глава 4. Информатизация, информационные системы, технологии и средства их обеспечения**

**Статья 16. Разработка и производство информационных систем, технологий и средств их обеспечения**

1. Все виды производства информационных систем и сетей, технологий и средств их обеспечения составляют специальную отрасль экономической деятельности, развитие которой определяется государственной научно-технической и промышленной политикой информатизации.
2. Государственные и негосударственные организации, а также граждане имеют равные права на разработку и производство информационных систем, технологий и средств их обеспечения.
3. Государство создает условия для проведения научно-исследовательских и опытно-конструкторских работ в области разработки и производства информационных систем, технологий и средств их обеспечения.
Правительство Российской Федерации определяет приоритетные направления развития информатизации и устанавливает порядок их финансирования.
4. Разработка и эксплуатация федеральных информационных систем финансируются из средств федерального бюджета по статье расходов «Информатика» («Информационное обеспечение»).

5. Органы государственной статистики совместно с Комитетом при Президенте Российской Федерации по политике информатизации устанавливают правила учета и анализа состояния отрасли экономической деятельности, развитие которой определяется государственной научно-технической и промышленной политикой информатизации.

**Статья 17. Право собственности на информационные системы, технологии и средства их обеспечения**

1. Информационные системы, технологии и средства их обеспечения могут быть объектами собственности физических и юридических лиц, государства.

2. Собственником информационной системы, технологии и средств их обеспечения признается физическое или юридическое лицо, на средства которого эти объекты произведены, приобретены или получены в порядке наследования, дарения или иным законным способом.

3. Информационные системы, технологии и средства их обеспечения включаются в состав имущества субъекта, осуществляющего права собственника или владельца этих объектов. Информационные системы, технологии и средства их обеспечения выступают в качестве товара (продукции) при соблюдении исключительных прав их разработчиков.

Собственник информационной системы, технологии и средств их обеспечения определяет условия использования этой продукции.

**Статья 18. Право авторства и право собственности на информационные системы, технологии и средства их обеспечения**

Право авторства и право собственности на информационные системы, технологии и средства их обеспечения могут принадлежать разным лицам.

О защите авторских и смежных прав см. также Закон РФ от 9 июля 1993 г. No 5351-1 «Об авторских правах».

Собственник информационной системы, технологии и средств их обеспечения обязан защищать права их автора в соответствии с законодательством Российской Федерации.

**Статья 19. Сертификация информационных систем, технологий, средств их обеспечения и лицензирование деятельности по формированию и использованию информационных ресурсов**

1. Информационные системы, базы и банки данных, предназначенные для информационного обслуживания граждан и организаций, подлежат сертификации в порядке, установленном Законом Российской Федерации «О сертификации продукции и услуг».

2. Информационные системы органов государственной власти Российской Федерации и органов государственной власти субъектов Российской Федерации, других государственных органов, организаций, которые обрабатывают документированную информацию с ограниченным доступом, а также средства защиты этих систем подлежат обязательной сертификации. Порядок сертификации определяется законодательством Российской Федерации.

3. Организации, выполняющие работы в области проектирования, производства средств защиты информации и обработки персональных данных, получают лицензии на этот вид деятельности. Порядок лицензирования определяется законодательством Российской Федерации.

4. Интересы потребителя информации при использовании импортной продукции в информационных системах защищаются таможенными органами Российской Федерации на основе международной системы сертификации.

**Глава 5. Защита информации и прав субъектов в области информационных процессов и информатизации**

**Статья 20. Цели защиты**

Целями защиты являются:

>• предотвращение утечки, хищения, утраты, искажения, подделки информации;

>• предотвращение угроз безопасности личности, общества, государства;

>• предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;
>• защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;
>• сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;
**>•** обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

**Статья 21. Защита информации**

1. Защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу.

Режим защиты информации устанавливается:

>• в отношении сведений, отнесенных к государственной тайне, — уполномоченными органами на основании Закона Российской Федерации «О государственной тайне»;
**>•** в отношении конфиденциальной документированной информации — собственником информационных ресурсов или уполномоченным лицом на основании настоящего Федерального закона;
>• в отношении персональных данных — Федеральным законом.

2. Органы государственной власти и организации, ответственные за формирование и использование информационных ресурсов, подлежащих защите, а также органы и организации, разрабатывающие и применяющие информационные системы и информационные технологии для формирования и использования информационных ресурсов с ограниченным доступом, руководствуются в своей деятельности законодательством Российской Федерации.

3. Контроль за соблюдением требований к защите информации и эксплуатацией специальных программно-технических средств защиты, а также обеспечение организационных мер защиты информационных систем, обрабатывающих информацию с ограниченным доступом в негосударственных структурах, осуществляются органами государственной власти. Контроль осуществляется в порядке, определяемом Правительством Российской Федерации.

4. Организации, обрабатывающие информацию с ограниченным доступом, которая является собственностью государства, создают специальные службы, обеспечивающие защиту информации.

5. Собственник информационных ресурсов или уполномоченные им лица имеют право осуществлять контроль за выполнением требований по защите информации и запрещать или приостанавливать обработку информации в случае невыполнения этих требований.

6. Собственник или владелец документированной информации вправе обращаться в органы государственной власти для оценки правильности выполнения норм и требований по защите его информации в информационных системах. Соответствующие органы определяет Правительство Российской Федерации. Эти органы соблюдают условия конфиденциальности самой информации и результатов проверки.

О защите информации, которой обмениваются Российская Федерация и НАТО, см. постановление Правительства РФ от 3 марта 1997 г. Ц-М 242.

**Статья 22. Права и обязанности субъектов в области защиты информации**

1. Собственник документов, массива документов, информационных систем или уполномоченные им лица в соответствии с настоящим Федеральным

законом устанавливают порядок предоставления пользователю информации с указанием места, времени, ответственных должностных лиц, а также необходимых процедур и обеспечивают условия доступа пользователей к информации.
2. Владелец документов, массива документов, информационных систем обеспечивает уровень защиты информации в соответствии с законодательством Российской Федерации.
3. Риск, связанный с использованием несертифицированных информационных систем и средств их обеспечения, лежит на собственнике (владельце) этих систем и средств.
Риск, связанный с использованием информации, полученной из несертифицированной системы, лежит на потребителе информации.
4. Собственник документов, массива документов, информационных систем может обращаться в организации, осуществляющие сертификацию средств защиты информационных систем и информационных ресурсов, для проведения анализа достаточности мер защиты его ресурсов и систем и получения консультаций.
5. Владелец документов, массива документов, информационных систем обязан оповещать собственника информационных ресурсов и (или) информационных систем о всех фактах нарушения режима защиты информации.

**Статья 23. Защита прав субъектов в сфере информационных процессов и информатизации**

1. Защита прав субъектов в сфере формирования информационных ресурсов, пользования информационными ресурсами, разработки, производства и применения информационных систем, технологий и средств их обеспечения осуществляется в целях предупреждения правонарушений, пресечения неправомерных действий, восстановления нарушенных прав и возмещения причиненного ущерба.
2. Защита прав субъектов в указанной сфере осуществляется судом, арбитражным судом, третейским судом с учетом специфики правонарушений и нанесенного ущерба.
3. За правонарушения при работе с документированной информацией органы государственной власти, организации и их должностные лица несут ответственность в соответствии с законодательством Российской Федерации и субъектов Российской Федерации.
Для рассмотрения конфликтных ситуаций и защиты прав участников в сфере формирования и использования информационных ресурсов, создания и использования информационных систем, технологий и средств их обеспечения могут создаваться временные и постоянные третейские суды.
Третейский суд рассматривает конфликты и споры сторон в порядке, установленном законодательством о третейских судах.
4. Ответственность за нарушения международных норм и правил в области формирования и использования информационных ресурсов, создания и использования информационных систем, технологий и средств их обеспечения возлагается на органы государственной власти, организации и граждан в соответствии с договорами, заключенными ими с зарубежными фирмами и другими партнерами с учетом международных договоров, ратифицированных Российской Федерацией.

**Статья 24. Защита права на доступ к информации**

1. Отказ в доступе к открытой информации или предоставление пользователям заведомо недостоверной информации могут быть обжалованы в судебном порядке.
Неисполнение или ненадлежащее исполнение обязательств по договору поставки, купли-продажи, по другим формам обмена информационными ресурсами между организациями рассматриваются арбитражным судом.
Во всех случаях лица, которым отказано в доступе к информации, и лица, получившие недостоверную информацию, имеют право на возмещение

понесенного ими ущерба.
2. Суд рассматривает споры о необоснованном отнесении информации к категории информации с ограниченным доступом, иски о возмещении ущерба в случаях необоснованного отказа в предоставлении информации пользователям или в результате других нарушений прав пользователей.
3. Руководители, другие служащие органов государственной власти, организаций, виновные в незаконном ограничении доступа к информации и нарушении режима защиты информации, несут ответственность в соответствии с уголовным, гражданским законодательством и законодательством об административных правонарушениях.

**Статья 25. Вступление в силу настоящего Федерального закона**

1. Настоящий Федеральный закон вступает в силу со дня его официального опубликования.
2. Предложить Президенту Российской Федерации привести в соответствие с настоящим Федеральным законом изданные им правовые акты.
3. Поручить Правительству Российской Федерации:
>• привести в соответствие с настоящим Федеральным законом изданные им правовые акты;
**>•** подготовить и внести в Государственную Думу в трехмесячный срок в установленном порядке предложения о внесении изменений и дополнений в законодательство Российской Федерации в связи с принятием настоящего Федерального закона;
>• принять нормативные правовые акты, обеспечивающие реализацию настоящего Федерального закона.

**Москва, Кремль**
**20 февраля 1995 г.**
**Президент Российской Федерации Б. Ельцин**

«О ГОСУДАРСТВЕННОЙ ТАЙНЕ»

**Закон РФ от 21 июля 1993 г. № 5485-1 (с изменениями от 6 октября 1997 г.)**

Постановление ВС РФ от 21 июля 1993 г. № 5486-1 «О порядке введения в действие Закона Российской Федерации «О государственной тайне».
Федеральным законом от 6 октября 1997 г. № 131-ФЗ в тексте настоящего Закона слова «Министерство безопасности Российской Федерации» заменены словами «Федеральная служба безопасности Российской Федерации» в соответствующих падежах, преамбула Закона после слова «их» дополнена словами «засекречиванием или».
Настоящий Закон регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

**Раздел I. Общие Положения**

О соответствии Конституции статьи 1 настоящего Закона см. Постановление Конституционного Суда РФ от 27 марта 1996 г. № 8-П.
Федеральным законом от 6 октября 1997 г. № 131-ФЗ в статье 1 настоящего Закона слово «представительной» заменено словом «законодательной».

**Статья 1. Сфера действия настоящего Закона**

Положения настоящего Закона обязательны для исполнения на территории Российской Федерации и за ее пределами органами законодательной, исполнительной и судебной властей (далее — органы государственной власти), местного самоуправления, предприятиями, учреждениями и организациями независимо от их организационно — правовой формы и формы собственности, должностными лицами и гражданами Российской Федерации, взявшими на себя обязательства либо обязанными по своему статусу исполнять требования законодательства Российской Федерации о государственной тайне.

**Статья 2. Основные понятия, используемые в настоящем Законе**

В настоящем Законе используются следующие основные понятия:
>• государственная тайна — защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;
>• носители сведений, составляющих государственную тайну, — материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов;
>• система защиты государственной тайны — совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну и их носителей, а также мероприятий, проводимых в этих целях;
>• допуск к государственной тайне — процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций — на проведение работ с использованием таких сведений;
>• доступ к сведениям, составляющим государственную тайну, — санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну;
>• гриф секретности — реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него;
**>•** средства защиты информации — технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации;
Федеральным законом от б октября 1997 г. № 131-ФЗ статья 2 настоящего Закона дополнена абзацем девятым следующего содержания:
>• перечень сведений, составляющих государственную тайну, — совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством.

**Статья 3. Законодательство Российской Федерации о государственной тайне**

Законодательство Российской Федерации о государственной тайне основывается на Конституции Российской Федерации, Законе Российской Федерации «О безопасности» и включает настоящий Закон, а также положения других актов законодательства, регулирующих отношения, связанные с защитой государственной тайны.
Федеральным законом от 6 октября 1997 г. No 131-ФЗ в статью 4 настоящего Закона внесены изменения, см. текст статьи в предыдущей редакции.

**Статья 4. Полномочия органов государственной власти и должностных лиц в области отнесения сведений к государственной тайне и их защиты**

1. Палаты Федерального Собрания:
**>•** осуществляют законодательное регулирование отношений в области государственной тайны;
**>•** рассматривают статьи федерального бюджета в части средств, направляемых на реализацию государственных программ в области защиты государственной тайны;
>• определяют полномочия должностных лиц в аппаратах палат Федерального Собрания по обеспечению защиты государственной тайны в палатах Федерального Собрания.
2. Президент Российской Федерации:
>• утверждает государственные программы в области защиты государственной тайны;

(Государственная программа обеспечена защиты государственной тайны в Российской Федерации на 1996—1997 гг. утверждена Указом Президента РФ от 9 марта 1996 г. № 346.)
>• утверждает по представлению Правительства Российской Федерации состав, структуру межведомственной комиссии по защите государственной тайны и положение о ней;
(Межведомственная комиссия по защите государственной тайны образована Указом Президента РФ от 8 ноября 1995 г. № 1108.
Положение о Межведомственной комиссии по защите государственной тайны утверждено Указом Президента РФ от 20 января 1996 г. № 71.
Персональный состав Межведомственной комиссии по защите государственной тайны утвержден постановлением Правительства РФ **от** 28 февраля 1996 г. № 203.)
>• утверждает по представлению Правительства Российской Федерации Перечень должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне, а также Перечень сведений, отнесенных к государственной тайне;
(Перечень должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне, Утвержден распоряжением Президента РФ от 30 мая 1997 г. No 226-рп.)
>• заключает международные договоры Российской Федерации о совместном использовании и защите сведений, составляющих государственную тайну;
>• определяет полномочия должностных лиц по обеспечению защиты государственной тайны в Администрации Президента Российской Федерации;
>• в пределах своих полномочий решает иные вопросы, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и их защитой.
3. Правительство Российской Федерации:
>• организует исполнение Закона Российской Федерации «О государственной тайне»;
>• представляет на утверждение Президенту Российской Федерации состав, структуру межведомственной комиссии по защите государственной тайны и положение о ней;
>• представляет на утверждение Президенту Российской Федерации Перечень должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне;
>• устанавливает порядок разработки Перечня сведений, отнесенных к государственной тайне;
>• организует разработку и выполнение государственных программ в области защиты государственной тайны;
>• определяет полномочия должностных лиц по обеспечению защиты государственной тайны в аппарате Правительства Российской Федерации;
>• устанавливает размеры и порядок предоставления льгот гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны;
(Порядок и условия выплаты процентных надбавок к должностному окладу (тарифной ставке) должностных лиц и граждан, допущенных к государственной тайне утверждены постановлением Правительства РФ от 14 октября 1994 г. Ns 1161.)
>• устанавливает порядок определения размеров ущерба, наступившего в результате несанкционированного распространения сведений, составляющих государственную тайну, а также ущерба, наносимого собственнику информации в результате ее засекречивания;
>• заключает межправительственные соглашения, принимает меры по выполнению международных договоров Российской Федерации о совместном использовании и защите сведений, составляющих государственную тайну, принимает решения о возможности передачи их носителей другим

государствам;
>• в пределах своих полномочий решает иные вопросы, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и их защитой.
4. Органы государственной власти Российской Федерации, органы государственной власти субъектов Российской Федерации и органы местного самоуправления во взаимодействии с органами защиты государственной тайны, расположенными в пределах соответствующих территорий:
>• обеспечивают защиту переданных им другими органами государственной власти, предприятиями, учреждениями и организациями сведений, составляющих государственную тайну, а также сведений, засекречиваемых ими;
>• обеспечивают защиту государственной тайны на подведомственных им предприятиях, в учреждениях и организациях в соответствии с требованиями актов законодательства Российской Федерации;
**>•** обеспечивают в пределах своей компетенции проведение проверочных мероприятий в отношении граждан, допускаемых к государственной тайне;
**>•** реализуют предусмотренные законодательством меры по ограничению прав граждан и предоставлению льгот лицам, имеющим либо имевшим доступ к сведениям, составляющим государственную тайну;
>• вносят в полномочные органы государственной власти предложения по совершенствованию системы защиты государственной тайны.
5. Органы судебной власти:
**>•** рассматривают уголовные и гражданские дела о нарушениях законодательства Российской Федерации о государственной Тайне;
>• обеспечивают судебную защиту граждан, органов государственной ' власти, предприятий, учреждений и организаций в связи с их деятельностью по защите государственной тайны;
>• обеспечивают в ходе рассмотрения указанных дел защиту государственной тайны;
>• определяют полномочия должностных лиц по обеспечению защиты государственной тайны в органах судебной власти.
Федеральным законом от 6 октября 1997 г. № 131-ФЗ название раздела II изложено в новой редакции, см. текст названия в предыдущей редакции.

**Раздел П. Перечень сведений, составляющих государственную тайну**

Федеральным законом от 6 октября 1997 г. № 131-ФЗ статья 5 настоящего Закона изложена в новой редакции, см. текст статьи в предыдущей редакции.

**Статья 5. Перечень сведений, составляющих государственную тайну**

Государственную тайну составляют:
1) сведения в военной области: о содержании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций, стратегическому, оперативному и мобилизационному развертыванию Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, предусмотренных Федеральным законом «Об обороне», об их боевой и мобилизационной готовности, о создании и об использовании мобилизационных ресурсов; о планах строительства Вооруженных Сил Российской Федерации, других войск Российской Федерации, о направлениях развития вооружения и военной техники, о содержании и результатах выполнения целевых программ, научно-исследовательских и опытно-конструкторских работ по созданию и модернизации образцов вооружения и военной техники; о разработке, технологии, производстве, об объемах производства, о хранении, об утилизации ядерных боеприпасов, их составных частей, делящихся ядерных материалов, используемых в ядерных боеприпасах, о технических средствах и (или) методах защиты ядерных боеприпасов от несанкционированного применения, а также о ядерных энергетических и специальных физических

установках оборонного значения; о тактико-технических характеристиках и возможностях боевого применения образцов вооружения и военной техники, о свойствах, рецептурах или технологиях производства новых видов ракетного топлива или взрывчатых веществ военного назначения; о дислокации, назначении, степени готовности, защищенности режимных и особо важных объектов, об их проектировании, строительстве и эксплуатации, а также об отводе земель, недр и акваторий для этих объектов; о дислокации, действительных наименованиях, об организационной структуре, о вооружении, численности войск и состояния их боевого обеспечения, а также о военно-политической и (или) оперативной обстановке;

2) сведения в области экономики, науки и техники: о содержании планов подготовки Российской Федерации и ее отдельных регионов к возможным военным действиям, о мобилизационных мощностях промышленности по изготовлению и ремонту вооружения и военной техники, об объемах производства, поставок, о запасах стратегических видов сырья и материалов, а также о размещении, фактических размерах и об использовании государственных материальных резервов; об использовании инфрастуктуры Российской Федерации в целях обеспечения обороноспособности и безопасности государства; о силах и средствах гражданской обороны, о дислокации, предназначении и степени защищенности объектов административного управления, о степени обеспечения безопасности населения, о функционировании транспорта и связи в Российской Федерации в целях обеспечения безопасности государства; об объемах, о планах (заданиях) государственного оборонного заказа, о выпуске и поставках (в денежном или натуральном выражении) вооружения, военной техники и другой оборонной продукции, о наличии и наращивании мощностей по их выпуску, о связях предприятий по кооперации, о разработчиках или об изготовителях указанных вооружения, военной техники и другой оборонной продукции;

о достижениях науки и техники, о научно-исследовательских, об опытно-конструкторских, о проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства; об объемах запасов, добычи, передачи и потребления платины, металлов платиновой группы, природных алмазов, а также об объемах других стратегических видов полезных ископаемых Российской Федерации (по списку, определяемому Правительством Российской Федерации);

3) сведения в области внешней политики и экономики: о внешнеполитической, внешнеэкономической деятельности Российской Федерации, преждевременное распространение которых может нанести ущерб безопасности государства; о финансовой политике в отношении иностранных государств (за исключением обобщенных показателей по внешней задолженности), а также о финансовой или денежно-кредитной деятельности, преждевременное распространение которых может нанести ущерб безопасности государства;

4) сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности: о силах, средствах, об источниках, о методах, планах и результатах разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения; о лицах, сотрудничающих или сотрудничавших на конфиденциальной основе с органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность; об организации, о силах, средствах и методах обеспечения безопасности объектов государственной охраны, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения; о системе президентской,

правительственной, шифрованной, в том числе кодированной и засекреченной связи, о шифрах, о разработке, об изготовлении шифров и обеспечении ими, о методах и средствах анализа шифровальных средств и средств специальной защиты, об информационно-аналитических системах специального назначения; о методах и средствах защиты секретной информации; об организации и о фактическом состоянии защиты государственной тайны; о защите Государственной границы Российской Федерации, исключительной экономической зоны и континентального шельфа Российской Федерации; о расходах федерального бюджета, связанных с обеспечением обороны, безопасности государства и правоохранительной деятельности в Российской Федерации; о подготовке кадров, раскрывающие мероприятия, проводимые в целях обеспечения безопасности государства.

Федеральным законом от 6 октября 1997 г. № 131-ФЗ название раздела III изложено в новой редакции, см. текст названия в предыдущей редакции.

**Раздел III. Отнесение сведений к государственной тайне и их засекречивание**

Федеральным законом от 6 октября 1997 г. Ns 131-ФЗ в статью б настоящего Закона внесены изменения, см. текст статьи в предыдущей редакции.

**Статья 6. Принципы отнесения сведений к государственной тайне и засекречивания этих сведений**

Отнесение сведений к государственной тайне и их засекречивание — введение в предусмотренном настоящим Законом порядке для сведений, составляющих государственную тайну, ограничений на их распространение и на доступ к их носителям.

Отнесение сведений к государственной тайне и их засекречивание осуществляется в соответствии с принципами законности, обоснованности и своевременности.

Законность отнесения сведений к государственной тайне и их засекречивание заключается в соответствии засекречиваемых сведений положениям статей 5 и 7 настоящего Закона и законодательству Российской Федерации о государственной тайне.

Обоснованность отнесения сведений к государственной тайне и их засекречивание заключается в установлении путем экспертной оценки целесообразности засекречивания конкретных сведений, вероятных экономических и иных последствий этого акта исходя из баланса жизненно важных интересов государства, общества и граждан.

Своевременность отнесения сведений к государственной тайне и их засекречивание заключается в установлении ограничений на распространение этих сведений с момента их получения (разработки) или заблаговременно.

Федеральным законом от 6 октября 1997 г. NB 131-ФЗ в статью 7 настоящего Закона внесены изменения, см. текст статьи в предыдущей редакции.

**Статья 7. Сведения, не подлежащие отнесению к государственной тайне и засекречиванию**

Не подлежат отнесению к государственной тайне и засекречиванию сведения:

>• о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;

>• о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;

>• о привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;

**>•** о фактах нарушения прав и свобод человека и гражданина;

>• о размерах золотого запаса и государственных валютных резервах

Российской Федерации;

>• о состоянии здоровья высших должностных лиц Российской Федерации;

>• о фактах нарушения законности органами государственной власти и их должностными лицами.

Должностные лица, принявшие решение о засекречивании перечисленных сведений либо о включении их в этих целях в носители сведений, составляющих государственную тайну, несут уголовную, административную или дисциплинарную ответственность в зависимости от причиненного обществу, государству и гражданам материального и морального ущерба. Граждане вправе обжаловать такие решения в суд.

О сведениях, не подлежащих засекречиванию, см. также постановление Правительства РФ от 7 августа 1995 г. № 798.

**Статья 8. Степени секретности сведений и грифы секретности носителей этих сведений**

Степень секретности сведений, составляющих государственную тайну, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения указанных сведений.

Устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: «особой важности», «совершенно секретно» и «секретно».

Порядок определения размеров ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения сведений, составляющих государственную тайну, и правила отнесения указанных сведений к той или иной степени секретности устанавливаются Правительством Российской Федерации.

Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности утверждены постановлением Правительства РФ от 4 сентября 1995 г. № 870.

Использование перечисленных грифов секретности для засекречивания сведений, не отнесенных к государственной тайне, не допускается.

Федеральным законом от 6 октября 1997 г. № 131-ФЗ в статью 9 настоящего Закона внесены изменения, см. текст статьи в предыдущей редакции.

**Статья 9. Порядок отнесения сведений к государственной тайне**

Отнесение сведений к государственной тайне осуществляется в соответствии с их отраслевой, ведомственной или программно-целевой принадлежностью, а также в соответствии с настоящим Законом.

Обоснование необходимости отнесения сведений к государственной тайне в соответствии с принципами засекречивания сведений возлагается на органы государственной власти, предприятия, учреждения и организации, которыми эти сведения получены (разработаны).

Отнесение сведений к государственной тайне осуществляется в соответствии с Перечнем сведений, составляющих государственную тайну, определяемым настоящим Законом, руководителями органов государственной власти в соответствии с Перечнем должностных лиц, наделенных полномочиями по отнесению сведений к государственной тайне, утверждаемым Президентом Российской Федерации. Указанные лица несут персональную ответственность за принятые ими решения о целесообразности отнесения конкретных сведений к государственной тайне.

Для осуществления единой государственной политики в области засекречивания сведений межведомственная комиссия по защите государственной тайны формирует по предложениям органов государственной власти и в соответствии с Перечнем сведений, составляющих государственную тайну, Перечень сведений, отнесенных к государственной тайне. В этом Перечне указываются органы государственной власти, наделяемые полномочиями по распоряжению данными сведениями. Указанный

Перечень утверждается Президентом Российской Федерации, подлежит открытому опубликованию и пересматривается по мере необходимости.
Органами государственной власти, руководители которых наделены полномочиями по отнесению сведений к государственной тайне, в соответствии с Перечнем сведений, отнесенных к государственной тайне, разрабатываются развернутые перечни сведений, подлежащих засекречиванию. В эти перечни включаются сведения, полномочиями по распоряжению которыми наделены указанные органы, и устанавливается степень их секретности. В рамках целевых программ по разработке и модернизации образцов вооружения и военной техники, опытно-конструкторских и научно-исследовательских работ по решению заказчиков указанных образцов и работ могут разрабатываться отдельные перечни сведений, подлежащих засекречиванию. Эти перечни утверждаются соответствующими руководителями органов государственной власти. Целесообразность засекречивания таких перечней определяется их содержанием.

**Статья 10. Ограничение прав собственности предприятий, учреждений организаций и граждан Российской Федерации на информацию в связи с ее засекречиванием**

Должностные лица, наделенные в порядке, предусмотренном статьей 9 настоящего Закона, полномочиями по отнесению сведений к государственной тайне, вправе принимать решения о засекречивании информации, находящейся в собственности предприятий, учреждений, организаций и граждан (далее - собственник информации), если эта информация включает сведения, перечисленные в Перечне сведений, отнесенных к государственной тайне. Засекречивание указанной информации осуществляется по представлению собственников информации или соответствующих органов государственной власти.
Материальный ущерб, наносимый собственнику информации в связи с ее засекречиванием, возмещается государством в размерах, определяемых в договоре между органом государственной власти, в распоряжение которого переходит эта информация, и ее собственником. В договоре также предусматриваются обязательства собственника информации по ее нераспространению.
При отказе собственника информации от подписания договора он предупреждается об ответственности за несанкционированное распространение сведений, составляющих государственную тайну в соответствии с действующим законодательством.
Собственник информации вправе обжаловать в суд действия должностных лиц, ущемляющие, по мнению собственника информации, его права. В случае признания судом действий должностных лиц незаконными порядок возмещения ущерба, нанесенного собственнику информации, определяется решением суда в соответствии с действующим законодательством.
Не может быть ограничено право собственности на информацию иностранных организаций и иностранных граждан, если эта информация получена (разработана) ими без нарушения законодательства Российской Федерации.

**Статья 11. Порядок засекречивания сведений и их носителей**

Основанием для засекречивания сведений, полученных (разработанных) в результате управленческой, производственной, научной и иных видов деятельности органов государственной власти, предприятий, учреждений и организаций, является их соответствие действующим в данных органах, на данных предприятиях, в данных учреждениях и организациях перечням сведений, подлежащих засекречиванию. При засекречивании этих сведений их носителям присваивается соответствующий гриф секретности.
При невозможности идентификации полученных (разработанных) сведений со сведениями, содержащимися в действующем перечне, должностные лица органов государственной власти, предприятий, учреждений и организаций

обязаны обеспечить предварительное засекречивание полученных (разработанных) сведений в соответствии с предполагаемой степенью секретности и в месячный срок направить в адрес должностного лица, утвердившего указанный перечень, предложения по его дополнению (изменению).

Должностные лица, утвердившие действующий перечень, обязаны в течение трех месяцев организовать экспертную оценку поступивших предложений и принять решение по дополнению (изменению) действующего перечня или снятию предварительно присвоенного сведениям грифа секретности.

**Статья 12. Реквизиты носителей сведений, составляющих государственную тайну**

На носители сведений, составляющих государственную тайну, наносятся реквизиты, включающие следующие данные:

**>•** о степени секретности содержащихся в носителе сведений со ссылкой на соответствующий пункт действующего в данном органе государственной власти, на данном предприятии, в данных учреждении и организации перечня сведений, подлежащих засекречиванию;

**>•** об органе государственной власти, о предприятии, об учреждении, организации, осуществивших засекречивание носителя;

>• о регистрационном номере;

>• о дате или условии рассекречивания сведений либо о событии, после наступления которого сведения будут рассекречены.

При невозможности нанесения таких реквизитов на носитель сведений, составляющих государственную тайну, эти данные указываются в сопроводительной документации на этот носитель.

Если носитель содержит составные части с различными степенями секретности, каждой из этих составных частей присваивается соответствующий гриф секретности, а носителю в целом присваивается гриф секретности, соответствующий тому грифу секретности, который присваивается его составной части, имеющей высшую для данного носителя степень секретности сведений.

Помимо перечисленных в настоящей статье реквизитов на носителе и (или) в сопроводительной документации к нему могут проставляться дополнительные отметки, определяющие полномочия должностных лиц по ознакомлению с содержащимися в этом носителе сведениями. Вид и порядок проставления дополнительных отметок и других реквизитов определяются нормативными документами, утверждаемыми Правительством Российской Федерации.

**Раздел IV. Рассекречивание сведений и их носителей**

О порядке рассекречивания архивных документов см. постановление Правительства РФ от 20 февраля 1995 г. № 170.

**Статья 13. Порядок рассекречивания сведений**

Рассекречивание сведений и их носителей — снятие ранее введенных в предусмотренном настоящим Законом порядке ограничений на распространение сведений, составляющих государственную тайну, и на доступ к их носителям.

Основаниями для рассекречивания сведений являются:

**>•** взятие на себя Российской Федерацией международных обязательств по открытому обмену сведениями, составляющими в Российской Федерации государственную тайну;

>• изменение объективных обстоятельств, вследствие которого дальнейшая защита сведений, составляющих государственную тайну, является нецелесообразной.

Органы государственной власти, руководители которых наделены полномочиями по отнесению сведений к государственной тайне, обязаны периодически, но не реже чем через каждые 5 лет, пересматривать содержание действующих в органах государственной власти, на

предприятиях, в учреждениях и организациях перечней сведений, подлежащих засекречиванию, в части обоснованности засекречивания сведений и их соответствия установленной ранее степени секретности.
Срок засекречивания сведений, составляющих государственную тайну, не должен превышать 30 лет. В исключительных случаях этот срок может быть продлен по заключению межведомственной комиссии по защите государственной тайны.
Правом изменения действующих в органах государственной власти, на предприятиях, в учреждениях и организациях перечней сведений, подлежащих засекречиванию, наделяются утвердившие их руководители органов государственной власти, которые несут персональную ответственность за обоснованность принятых ими решений по рассекречиванию сведений. Решения указанных руководителей, связанные с изменением перечня сведений, отнесенных к государственной тайне, подлежат согласованию с межведомственной комиссией по защите государственной тайны, которая вправе приостанавливать и опротестовывать эти решения.

**Статья 14. Порядок рассекречивания носителей сведений, составляющих государственную тайну**

Носители сведений, составляющих государственную тайну, рассекречиваются не позднее сроков, установленных при их засекречивании. До истечения этих сроков носители подлежат рассекречиванию, если изменены положения действующего в данном органе государственной власти, на предприятии, в учреждении и организации перечня, на основании которых они были засекречены.
В исключительных случаях право продления первоначально установленных сроков засекречивания носителей сведений, составляющих государственную тайну, предоставляется руководителям государственных органов, наделенным полномочиями по отнесению соответствующих сведений к государственной тайне, на основании заключения назначенной ими в установленном порядке экспертной комиссии.
Руководители органов государственной власти, предприятий, учреждений и организаций наделяются полномочиями по рассекречиванию носителей сведений, необоснованно засекреченных подчиненными им должностными лицами.
Руководители государственных архивов Российской Федерации наделяются полномочиями по рассекречиванию носителей сведений, составляющих государственную тайну, находящихся на хранении в закрытых фондах этих архивов, в случае делегирования им таких полномочий организацией — фондообразователем или ее правопреемником. В случае ликвидации организации — фондообразователя и отсутствия ее правопреемника вопрос о порядке рассекречивания носителей сведений, составляющих государственную тайну, рассматривается межведомственной комиссией по защите государственной тайны.

**Статья 15. Исполнение запросов граждан, предприятий, учреждений, организаций и органов государственной власти Российской Федерации о рассекречивании сведений**

Граждане, предприятия, учреждения, организации и органы государственной власти Российской Федерации вправе обратиться в органы государственной власти, на предприятия, в учреждения, организации в том числе в государственные архивы, с запросом о рассекречивании сведений, отнесенных к государственной тайне.
Органы государственной власти, предприятия, учреждения, организации, в том числе государственные архивы, получившие такой запрос, обязаны в течение трех месяцев рассмотреть его и дать мотивированный ответ по существу запроса. Если они не правомочны решить вопрос о рассекречивании запрашиваемых сведений, то запрос в месячный срок с

момента его поступления передается в орган государственной власти, наделенный такими полномочиями либо в межведомственную комиссию по защите государственной тайны о чем уведомляются граждане предприятия, учреждения, организации и органы государственной власти Российской Федерации, подавшие запрос.

Уклонение должностных лиц от рассмотрения запроса по существу влечет за собой административную (дисциплинарную) ответственность в соответствии с действующим законодательством.

Обоснованность отнесения сведений к государственной тайне может быть обжалована в суд. При признании судом необоснованности засекречивания сведений эти сведения подлежат рассекречиванию в установленном настоящим Законом порядке.

**Раздел V. Распоряжение сведениями, составляющими государственную тайну**

**Статья 16. Взаимная передача сведений, составляющих государственную тайну, органами государственной власти, предприятиями, учреждениями и организациями**

Взаимная передача сведений, составляющих государственную тайну, осуществляется органами государственной власти, предприятиями, учреждениями и организациями, не состоящими в отношениях подчиненности и не выполняющими совместных работ с санкции органа государственной власти, в распоряжении которого в соответствии со статьей 9 настоящего Закона находятся эти сведения.

Органы государственной власти, предприятия, учреждения и организации, запрашивающие сведения, составляющие государственную тайну, обязаны создать условия, обеспечивающие защиту этих сведений. Их руководители несут персональную ответственность за несоблюдение установленных ограничений по ознакомлению со сведениями, составляющими государственную тайну.

Обязательным условием для передачи сведений, составляющих государственную тайну, органам государственной власти, предприятиям, учреждениям и организациям является выполнение ими требований, предусмотренных в статье 27 настоящего Закона.

Постановлением ВС РФ от 21 июля 1993 г. № 5486-1 установлено, что часть первая статьи 17 настоящего Закона вводится в действие не позднее 1 января 1995 года.

**Статья 17. Передача сведений, составляющих государственную тайну, в связи с выполнением совместных и других работ**

Передача сведений, составляющих государственную тайну, предприятиям, учреждениям, организациям или гражданам в связи с выполнением совместных и других работ осуществляется заказчиком этих работ с разрешения органа государственной власти, в распоряжении которого в соответствии со статьей 9 настоящего Закона находятся соответствующие сведения, и только в объеме, необходимом для выполнения этих работ. При этом до передачи сведений, составляющих государственную тайну, заказчик обязан убедиться в наличии у предприятия, учреждения или организации лицензии на проведение работ с использованием сведений соответствующей степени секретности, а у граждан — соответствующего допуска.

Предприятия, учреждения или организации, в том числе и негосударственных форм собственности, при проведении совместных и других работ (получении государственных заказов) и возникновении в связи с этим необходимости в использовании сведений, составляющих государственную тайну, могут заключать с государственными предприятиями, учреждениями или организациями договоры об использовании услуг их структурных подразделений по защите государственной тайны, о чем делается соответствующая отметка в лицензиях на проведение работ с использованием сведений, составляющих государственную тайну, обеих договаривающихся сторон.

В договоре на проведение совместных и других работ, заключаемом в установленном законом порядке, предусматриваются взаимные обязательства сторон по обеспечению сохранности сведений, составляющих государственную тайну, как в процессе проведения работ, так и по их завершении, а также условия финансирования работ (услуг) по защите сведений, составляющих государственную тайну.

Организация контроля за эффективностью защиты государственной тайны при проведении совместных и других работ возлагается на заказчика этих работ в соответствии с положениями заключенного сторонами договора.

При нарушении исполнителем в ходе совместных и других работ взятых на себя обязательств по защите государственной тайны заказчик вправе приостановить выполнение заказа до устранения нарушений, а при повторных нарушениях — поставить вопрос об аннулировании заказа и лицензии на проведение работ с использованием сведений, составляющих государственную тайну, и о привлечении виновных лиц к ответственности. При этом материальный ущерб, нанесенный исполнителем государству в лице заказчика, подлежит взысканию в соответствии с действующим законодательством.

**Статья 18. Передача сведений, составляющих государственную тайну, другим государствам**

Решение о передаче сведений, составляющих государственную тайну, другим государствам принимается Правительством Российской Федерации при наличии экспертного заключения межведомственной комиссии по защите государственной тайны о возможности передачи этих сведений.

См. Положение о подготовке к передаче сведений, составляющих государственную тайну, другим государствам, утвержденное постановлением Правительства РФ от 2 августа 1997 г. № 973.

Обязательства принимающей стороны по защите передаваемых ей сведений предусматриваются заключаемым с ней договором (соглашением).

**Статья 19. Защита сведений, составляющих государственную тайну, при изменении функций субъектов правоотношений**

Органы государственной власти, предприятия, учреждения и организации, располагающие сведениями, составляющими государственную тайну, в случаях изменения их функций, форм собственности, ликвидации или прекращения работ с использованием сведений, составляющих государственную тайну, обязаны принять меры по обеспечению защиты этих сведений и их носителей. При этом носители сведений, составляющих государственную тайну, в установленном порядке уничтожаются, сдаются на архивное хранение либо передаются:

>• правопреемнику органа государственной власти, предприятия, учреждения или организации, располагающих сведениями, составляющими государственную тайну, если этот правопреемник имеет полномочия по проведению работ с использованием указанных сведений;

**>•** органу государственной власти, в распоряжении которого в соответствии со статьей 9 настоящего Закона находятся соответствующие сведения;

>• другому органу государственной власти, предприятию, учреждению или организации по указанию межведомственной комиссии по защите государственной тайны.

**Раздел VI. Защита государственной тайны**

**Статья 20. Органы защиты государственной тайны**

К органам защиты государственной тайны относятся:

>• межведомственная комиссия по защите государственной тайны;

>• органы федеральной исполнительной власти (Федеральная служба безопасности Российской Федерации, Министерство обороны Российской Федерации, Федеральное агентство правительственной связи и информации при Президенте Российской Федерации), Служба внешней разведки

Российской Федерации, Государственная техническая комиссия при Президенте Российской Федерации и их органы на местах;
>• органы государственной власти, предприятия, учреждения и организации и их структурные подразделения по защите государственной тайны.
Межведомственная комиссия по защите государственной тайны является коллегиальным органом, координирующим деятельность органов государственной власти по защите государственной тайны в интересах разработки и выполнения государственных программ нормативных и методических документов, обеспечивающих реализацию законодательства Российской Федерации о государственной тайне. Функции межведомственной комиссии по защите государственной тайны и ее надведомственные полномочия реализуются в соответствии с Положением о межведомственной комиссии по защите государственной тайны, утверждаемым Президентом Российской Федерации.
Указом Президента РФ от 30 марта 1994 г. № 614 функции межведомственной комиссии по защите государственной тайны временно возложены на Государственную техническую комиссию при Президенте Российской Федерации.
Органы федеральной исполнительной власти (Федеральная служба безопасности Российской Федерации, Министерства обороны Российской Федерации, Федеральное агентство правительственной связи и информации при Президенте Российской Федерации), Служба внешней разведки Российской Федерации, Государственная техническая комиссия при Президенте Российской Федерации и их органы на местах организуют и обеспечивают защиту государственной тайны в соответствии с функциями, возложенными на них законодательством Российской Федерации.
Органы государственной власти, предприятия, учреждения и организации обеспечивают защиту сведений, составляющих государственную тайну, в соответствии с возложенными на них задачами и в пределах своей компетенции. Ответственность за организацию защиты сведений, составляющих государственную тайну, в органах государственной власти, на предприятиях в учреждениях и организациях возлагается на их руководителей. В зависимости от объема работ с использованием сведений, составляющих государственную тайну, руководителями органов государственной власти предприятий, учреждений и организаций создаются структурные подразделения по защите государственной тайны, функции которых определяются указанными руководителями в соответствии с нормативными документами, утверждаемыми Правительством Российской Федерации, и с учетом специфики проводимых ими работ.
Защита государственной тайны является видом основной деятельности органа государственной власти, предприятия, учреждения или организации.
Постановлением Правительства РФ от 3 марта 1997 г. № 242 на федеральную службу безопасности Российской Федерации возложено выполнение функций органа Российской Федерации, ответственного за осуществление мероприятий и процедур в области защиты информации и обеспечение надзора в целях защиты информации, имеющей гриф секретности, которой обмениваются Российская Федерация и НАТО.
О соответствии Конституции статьи 21 настоящего Закона см. постановление Конституционного Суда РФ от 27 марта 1996 г. № 8-П.

**Статья 21. Допуск должностных лиц и граждан к государственной тайне**

Допуск должностных лиц и граждан Российской Федерации к государственной тайне осуществляется в добровольном порядке.
Допуск лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне осуществляется в порядке, устанавливаемом Правительством Российской Федерации.
Допуск должностных лиц и граждан к государственной тайне

предусматривает:
>• принятие на себя обязательств перед государством по нераспространению доверенных им сведений, составляющих государственную тайну;
>• согласие на частичные, временные ограничения их прав в соответствии со статьей 24 настоящего Закона;
>• письменное согласие на проведение в отношении их полномочными органами проверочных мероприятий;
>• определение видов, размеров и порядка предоставления льгот, предусмотренных настоящим Законом;
**>•** ознакомление с нормами законодательства Российской Федераций О государственной тайне, предусматривающими ответственность за его нарушение;
>• принятие решения руководителем органа государственной власти, предприятия, учреждения или организации о допуске оформляемого лица к сведениям, составляющим государственную тайну. Объем проверочных мероприятий зависит от степени секретности сведений, к которым будет допускаться оформляемое лицо. Проверочные мероприятия осуществляются в соответствии с законодательством Российской Федерации. Целью проведения проверочных мероприятий является выявление оснований, предусмотренных статьей 22 настоящего Закона.
Для должностных лиц и граждан, допущенных к государственной тайне на постоянной основе, устанавливаются следующие льготы:
>• процентные надбавки к заработной плате в зависимости от степени секретности сведений, к которым они имеют доступ;
(Порядок и условия выплаты процентных надбавок к должностному окладу (тарифной ставке) должностных лиц и граждан, допущенных к государственной тайне утверждены постановлением Правительства РФ от 14 октября 1994 г. NB 1161.)
**>•** преимущественное право при прочих равных условиях на оставление на работе при проведении органами государственной власти, предприятиями, учреждениями и организациями организационных и (или) штатных мероприятий.
Для сотрудников структурных подразделений по защите государственной тайны дополнительно к льготам, установленным для должностных лиц и граждан, допущенных к государственной тайне на постоянной основе, устанавливается процентная надбавка к заработной плате за стаж работы в указанных структурных подразделениях.
Взаимные обязательства администрации и оформляемого лица отражаются в трудовом договоре (контракте). Заключение трудового договора (контракта) до окончания проверки компетентными органами не допускается.
Устанавливается три формы допуска к государственной тайне должностных лиц и граждан, соответствующие трем степеням секретности сведений, составляющих государственную тайну: к сведениям особой важности, совершенно секретным или секретным. Наличие у должностных лиц и граждан допуска к сведениям более высокой степени секретности является основанием для доступа их к сведениям более низкой степени секретности.
Сроки, обстоятельства и порядок переоформления допуска граждан к государственной тайне устанавливаются нормативными документами, утверждаемыми Правительством Российской Федерации.
См. Инструкцию о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне, утвержденную постановлением Правительства РФ от 28 октября 1995 г. № 1050.
Порядок допуска должностных лиц и граждан к государственной тайне в условиях объявленного чрезвычайного положения может быть изменен Президентом Российской Федерации.

Федеральным законом от 6 октября 1997 г. № 131-ФЗ настоящий Закон дополнен статьей 21(1).

**Статья 21(1). Особый порядок допуска к государственной тайне**

Члены Совета Федерации, депутаты Государственной Думы, судьи на период исполнения ими своих полномочий, а также адвокаты, участвующие в качестве защитников в уголовном судопроизводстве по делам, связанным со сведениями, составляющими государственную тайну, допускаются к сведениям, составляющим государственную тайну, без проведения проверочных мероприятий, предусмотренных статьей 21 настоящего Закона.

Указанные лица предупреждаются о неразглашении государственной тайны, ставшей им известной в связи с исполнением ими своих полномочий, и о привлечении их к ответственности в случае ее разглашения, о чем у них отбирается соответствующая расписка.

Сохранность государственной тайны в таких случаях гарантируется путем установления ответственности указанных лиц федеральным законом.

**Статья 22. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне**

Федеральным законом от 6 октября 1997 г. № 131-ФЗ в абзаце втором части первой статьи 22 настоящего Закона слова «особо опасным» исключены.

Основаниями для отказа должностному лицу или гражданину в допуске к государственной тайне могут являться:

>• признание его судом недееспособным, ограниченно дееспособным или особо опасным рецидивистом, нахождение его под судом или следствием за государственные и иные тяжкие преступления, наличие у него неснятой судимости за эти преступления;

>• наличие у него медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну, согласно перечню, утверждаемому Министерством здравоохранения Российской Федерации;

>• постоянное проживание его самого и (или) его близких родственников за границей и (или) оформление указанными лицами документов для выезда на постоянное жительство в другие государства;

**>•** выявление в результате проверочных мероприятий действий оформляемого лица, создающих угрозу безопасности Российской Федерации;

>• уклонение его от проверочных мероприятий и (или) сообщение им заведомо ложных анкетных данных.

Решение об отказе должностному лицу или гражданину в допуске к государственной тайне принимается руководителем органа государственной власти, предприятия, учреждения или организации в индивидуальном порядке с учетом результатов проверочных мероприятий. Гражданин имеет право обжаловать это решение в вышестоящую организацию или в суд.

**Статья 23. Условия прекращения допуска должностного лица или гражданина к государственной тайне**

Допуск должностного лица или гражданина к государственной тайне может быть прекращен по решению руководителя органа государственной власти, предприятия, учреждения или организации в случаях:

**>•** расторжения с ним трудового договора (контракта) в связи с проведением организационных и (или) штатных мероприятий;

>• однократного нарушения им взятых на себя предусмотренных трудовым договором (контрактом) обязательств, связанных с защитой государственной тайны;

>• возникновения обстоятельств, являющихся согласно статье 22 настоящего Закона основанием для отказа должностному лицу или гражданину в допуске к государственной тайне.

Прекращение допуска должностного лица или гражданина к государственной тайне является дополнительным основанием для расторжения с ним трудового договора (контракта), если такие условия предусмотрены в

трудовом договоре (контракте).
Прекращение допуска к государственной тайне не освобождает должностное лицо или гражданина от взятых ими обязательств по неразглашению сведений, составляющих государственную тайну.
Решение администрации о прекращении допуска должностного лица или гражданина к государственной тайне и расторжении на основании этого с ним трудового договора (контракта) может быть обжаловано в вышестоящую организацию или в суд.

**Статья 24. Ограничения прав должностного лица или гражданина, допущенных или ранее допускавшихся к государственной тайне**

Должностное лицо или гражданин, допущенные или ранее допускавшиеся к государственной тайне, могут быть временно ограничены в своих правах. Ограничения могут касаться:
>• права выезда за границу на срок, оговоренный в трудовом договоре (контракте) при оформлении допуска гражданина к государственной тайне;
>• права на распространение сведений, составляющих государственную тайну, и на использование открытий и изобретений, содержащих такие сведения;
>• права на неприкосновенность частной жизни при проведении проверочных мероприятий в период оформления допуска к государственной тайне.

**Статья 25. Организация доступа должностного лица или гражданина к сведениям, составляющим государственную тайну**

Организация доступа должностного лица или гражданина к сведениям, составляющим государственную тайну, возлагается на руководителя соответствующего органа государственной власти, предприятия, учреждения или организации, а также на их структурные подразделения по защите государственной тайны. Порядок доступа должностного лица или гражданина к сведениям, составляющим государственную тайну, устанавливается нормативными документами, утверждаемыми Правительством Российской Федерации.
Руководители органов государственной власти, предприятий, учреждений и организаций несут персональную ответственность за создание таких условий, при которых должностное лицо или гражданин знакомятся только с теми сведениями, составляющими государственную тайну, и в таких объемах, которые необходимы ему для выполнения его должностных (функциональных) обязанностей.

**Статья 26. Ответственность за нарушение законодательства Российской Федерации о государственной тайне**

Должностные лица и граждане, виновные в нарушении законодательства Российской Федерации о государственной тайне, несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством.
Федеральным законом от 6 октября 1997 г. № 131-ФЗ статья 26 настоящего Закона дополнена новой частью второй, часть вторая считается частью третьей.
Соответствующие органы государственной власти и их должностные лица основываются на подготовленных в установленном порядке экспертных заключениях об отнесении незаконно распространенных сведений к сведениям, составляющим государственную тайну.
Защита прав и законных интересов граждан, органов государственной власти, предприятий, учреждений и организаций в сфере действия настоящего Закона осуществляется в судебном или ином порядке, предусмотренном настоящим Законом.
Постановлением ВС РФ от 21 июля 1993 г. № 5486-1 установлено, что часть первая статьи 27 настоящего Закона вводится в действие не позднее 1 января 1995 г.

**Статья 27. Допуск предприятий, учреждений и организаций к проведению**

**работ, связанных с использованием сведений, составляющих государственную тайну**

Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны, осуществляется путем получения ими в порядке, устанавливаемом Правительством Российской Федерации, лицензий на проведение работ со сведениями соответствующей степени секретности.

Положение о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны утверждено постановлением Правительства РФ от 15 апреля 1995 г. № 333.

Лицензия на проведение указанных работ выдается на основании результатов специальной экспертизы предприятия, учреждения и организации и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих государственную тайну, расходы по проведению которых относятся на счет предприятия, учреждения, организации, получающих лицензию.

Лицензия на проведение работ с использованием сведений, составляющих государственную тайну, выдается предприятию, учреждению, организации при выполнении ими следующих условий:

>• выполнение требований нормативных документов, утверждаемых Правительством Российской Федерации, по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ, связанных с использованием указанных сведений;

>• наличие в их структуре подразделений по защите государственной тайны и специально подготовленных сотрудников для работы по защите информации, количество и уровень квалификации которых достаточны для обеспечения защиты государственной тайны;

>• наличие у них сертифицированных средств защиты информации.

**Статья 28. Порядок сертификации средств защиты информации**

Средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

Организация сертификации средств защиты информации возлагается на Государственную техническую комиссию при Президенте Российской Федерации, Федеральная служба безопасности Российской Федерации, Федеральное агентство правительственной связи и информации при Президенте Российской Федерации, Министерство обороны Российской Федерации в соответствии с функциями, возложенными на них законодательством Российской Федерации. Сертификация осуществляется на основании требований государственных стандартов Российской Федерации и иных нормативных документов, утверждаемых Правительством Российской Федерации.

Положение о сертификации средств защиты информации утверждено постановлением Правительства РФ от 26 июня 1995 г. NQ 608.

Координация работ по организации сертификации средств защиты информации возлагается на межведомственную комиссию по защите государственной тайны.

**Раздел VII. Финансирование мероприятий по защите государственной тайны**

**Статья 29. Финансирование мероприятий по защите государственной тайны**

Финансирование деятельности органов государственной власти, бюджетных предприятий, учреждений и организаций и их структурных подразделений по защите государственной тайны осуществляется за счет средств

соответствующих бюджетов, а остальных предприятий, учреждений и организаций — за счет средств, получаемых от их основной деятельности при выполнении работ, связанных с использованием сведений, составляющих государственную тайну.

Средства на финансирование государственных программ в области защиты государственной тайны предусматриваются в федеральном бюджете Российской Федерации отдельной строкой.

Контроль за расходованием финансовых средств, выделяемых на проведение мероприятий по защите государственной тайны, осуществляется руководителями органов государственной власти, предприятий, учреждений и организаций, заказчиками работ, а также специально уполномоченными на то представителями Министерства финансов Российской Федерации. Если осуществление этого контроля связано с доступом к сведениям, составляющим государственную, тайну, то перечисленные лица должны иметь допуск к сведениям соответствующей степени секретности.

**Раздел VIII. Контроль и надзор за обеспечением защиты государственной тайны**

Федеральным законом от 6 октября 1997 г. № 131-ФЗ статья 30 настоящего Закона изложена в новой редакции, см. текст статьи в предыдущей редакции.

**Статья 30. Контроль за обеспечением защиты государственной тайны**

Контроль за обеспечением защиты государственной тайны осуществляют Президент Российской Федерации, Правительство Российской Федерации в пределах полномочий», определяемых Конституцией Российской Федерации, федеральными конституционными законами и федеральными законами.

**Статья 31. Межведомственный и ведомственный контроль**

Межведомственный контроль за обеспечением защиты государственной тайны в органах государственной власти, на предприятиях, в учреждениях и организациях осуществляют органы федеральной исполнительной власти (Федеральная служба безопасности Российской Федерации, Министерство обороны Российской Федерации, федеральное агентство правительственной связи и информации при Президенте Российской Федерации), Служба внешней разведки Российской Федерации, Государственная техническая комиссия при Президенте Российской Федерации и их органы на местах, на которые эта функция возложена законодательством Российской Федерации.

Органы государственной власти, наделенные в соответствии с настоящим Законом полномочиями по распоряжению сведениями, составляющими государственную тайну, обязаны контролировать эффективность защиты этих сведений во всех подчиненных и подведомственных им органах государственной власти, на предприятиях, в учреждениях и организациях, осуществляющих работу с ними.

Федеральным законом от 6 октября 1997 г. № 131-ФЗ часть третья статьи 31 настоящего Закона изложена в новой редакции, см. текст части третьей в предыдущей редакции.

Контроль за обеспечением защиты государственной тайны в Администрации Президента Российской Федерации, в аппаратах палат Федерального Собрания, Правительства Российской Федерации организуется их руководителями.

Контроль за обеспечением защиты государственной тайны в судебных органах и органах прокуратуры организуется руководителями этих органов.

**Статья 32. Прокурорский надзор**

Надзор за соблюдением законодательства при обеспечении защиты государственной тайны и законностью принимаемых при этом решений осуществляют Генеральный прокурор Российской Федерации и подчиненные ему прокуроры.

Доступ лиц, осуществляющих прокурорский надзор, к сведениям, составляющим государственную тайну, осуществляется в соответствии со

статьей 25 настоящего Закона.

**Москва, Дом Советов России**

**21 июля 1993 г.**

**Президент Российской Федерации Б. Ельцин**

**«О ФЕДЕРАЛЬНЫХ ОРГАНАХ ПРАВИТЕЛЬСТВЕННОЙ СВЯЗИ И ИНФОРМАЦИИ»**

**Закон РФ от 19 февраля 1993 г. № 4524-1 (с изменениями от 24 декабря 1993 г.)**

Настоящий Закон определяет назначение, правовую основу, принципы организации и основные направления деятельности, систему, обязанности и права, силы и средства федеральных органов правительственной связи и информации, а также виды и порядок контроля и надзора за их деятельностью.

**Раздел I. Общие положения**

**Статья 1. Назначение федеральных органов правительственной связи и информации**

Федеральные органы правительственной связи и информации являются составной частью сил обеспечения безопасности Российской Федерации и входят в систему органов федеральной исполнительной власти.

Федеральные органы правительственной связи и информации обеспечивают высшие органы государственной власти Российской Федерации, органы государственной власти субъектов Российской Федерации, центральные органы федеральной исполнительной власти, Совет безопасности Российской Федерации (далее — государственные органы), организации, предприятия, учреждения специальными видами связи и информации, а также организуют деятельность центральных органов федеральной исполнительной власти, организаций, предприятий, учреждений по обеспечению криптографической и инженерно-технической безопасности шифрованной связи в Российской Федерации и ее учреждениях за рубежом, осуществляют государственный контроль за этой деятельностью.

Федеральные органы правительственной связи и информации в пределах своей компетенции участвуют с Главным управлением охраны Российской Федерации в организации и обеспечении президентской связи.

**Статья 2. Правовая основа деятельности федеральных органов правительственной связи и информации**

Правовую основу деятельности федеральных органов правительственной связи и информации составляют Конституция Российской Федерации, Законы Российской Федерации «О безопасности», «Об обороне», «О внешней разведке», настоящий Закон, другие законы Российской Федерации, а также принимаемые в соответствии с ними нормативные акты Президента Российской Федерации и Правительства Российской Федерации.

Деятельность федеральных органов правительственной связи и информации осуществляется в соответствии с международными договорами и соглашениями, заключенными либо признанными Российской Федерацией.

Федеральные органы правительственной связи и информации издают в соответствии с законодательством Российской Федерации нормативные акты в пределах своей компетенции.

Создание и деятельность политических партий и организаций в федеральных органах правительственной связи и информации не допускаются.

**Статья 3. Основные направления деятельности федеральных органов правительственной связи и информации**

Основными направлениями деятельности федеральных органов правительственной связи и информации являются:

**>•** организация и обеспечение эксплуатации, безопасности, развития и совершенствования правительственной связи, иных видов специальной связи и систем специальной информации для государственных органов;

**>•** обеспечение в пределах своей компетенции сохранности государственных секретов; организация и обеспечение криптографической и инженерно-

технической безопасности шифрованной связи в Российской Федерации и ее учреждениях за рубежом;
>• организация и ведение внешней разведывательной деятельности в сфере шифрованной, засекреченной и иных видов специальной связи с использованием радиоэлектронных средств и методов;
**>•** обеспечение высших органов государственной власти Российской Федерации, центральных органов федеральной исполнительной власти, Совета безопасности Российской Федерации достоверной и независимой от других источников специальной информацией (материалы внешней разведывательной деятельности, информация по поддержанию управления народным хозяйством в особый период, военное время и при чрезвычайных ситуациях, экономическая информация мобилизационного назначения, информация социально-экономического мониторинга), необходимой им для принятия решений в области безопасности, обороны, экономики, науки и техники, международных отношений, экологии, а также мобилизационной готовности.

**Статья 4. Принципы организации деятельности федеральных органов правительственной связи и информации**

1. Деятельность федеральных органов правительственной связи и информации строится на основе принципов:
>• законности;
**>•** уважения прав и свобод человека и гражданина;
**>•** сохранности государственных секретов;
>• подконтрольности и подотчетности высшим органам государственной власти Российской Федерации.
2. Федеральные органы правительственной связи и информации действуют на основе:
>• единства системы федеральных органов правительственной связи и информации;
>• централизации управления системой федеральных органов правительственной связи и информации;
**>•** сочетания линейного, территориального и объектового принципов организации деятельности федеральных органов правительственной связи и информации.

**Раздел II. Система федеральных органов правительственной связи и информации**

**Статья 5. Построение системы федеральных органов правительственной связи и информации**

Единую систему федеральных органов правительственной связи и информации составляют:
>• Федеральное агентство правительственной связи и информации при Президенте Российской Федерации (далее — Федеральное агентство);
**>•** органы правительственной связи и информации (центры правительственной связи, информационно-аналитические органы) в субъектах Российской Федерации;
>• войска;
>• учебные заведения, научно-исследовательские организации, предприятия.
Федеральные органы правительственной связи и информации создают структурные подразделения по финансовому, материально-техническому, инженерно-строительному, медицинскому и иному обеспечению своей деятельности.
При Федеральном агентстве действует Академия криптографии Российской Федерации.

**Статья 6. Федеральное агентство правительственной связи и информации при Президенте Российской Федерации**

1. Федеральное агентство находится в непосредственном ведении

Президента Российской Федерации и является центральным органом федеральной исполнительной власти, ведающим вопросами организации и обеспечения правительственной связи, иных видов специальной связи для государственных органов, организации и обеспечения криптографической и инженерно-технической безопасности шифрованной связи, организации и ведения разведывательной деятельности в сфере шифрованной, засекреченной и иных видов специальной связи, специального информационного обеспечения высших органов государственной власти Российской Федерации, центральных органов федеральной исполнительной власти. Возглавляет Федеральное агентство и руководит его деятельностью генеральный директор.

Подразделения и части радиоразведки Федерального агентства, обеспечивающие организацию и ведение разведывательной деятельности в сфере шифрованной, засекреченной и иных видов специальной связи, образуют орган внешней разведки Федерального агентства, руководимый генеральным директором и действующий в соответствии с Законом Российской Федерации «О внешней разведке».

2. Федеральное агентство осуществляет государственное регулирование и межотраслевую координацию по вопросам, находящимся в его ведении.

Нормативные акты, предписания Федерального агентства в части организации, обеспечения функционирования и безопасности правительственной, шифрованной и иных видов специальной связи обязательны для исполнения государственными органами, а также организациями, предприятиями, учреждениями независимо от их ведомственной принадлежности и организационно-правовых форм с учетом взаимно согласованных требований ведомственных инструкций по организации и обеспечению безопасности шифрованной связи.

Согласно Указу Президента РФ от 24 декабря 1993 г. № 2288 часть третья статьи б настоящего Указа не подлежит применению органами государственной власти, органами местного самоуправления и их должностными лицами в части согласования положений с комитетом Верховного Совета Российской Федерации и высшими должностными лицами субъектов Российской Федерации.

3. Задачи, функции, организация и структура Федерального агентства определяются Положением о Федеральном агентстве правительственной связи и информации при Президенте Российской Федерации, утверждаемым Президентом Российской Федерации по согласованию с Комитетом Верховного Совета Российской Федерации по вопросам обороны и безопасности.

4. Федеральное агентство организует, руководит и непосредственно проводит работу по направлениям деятельности федеральных органов правительственной связи и информации, издает приказы, указания, положения, инструкции и другие нормативные акты, обязательные для исполнения в системе федеральных органов правительственной связи и информации.

**Статья 7. Органы правительственной связи и информации в субъектах Российской Федерации**

Органы правительственной связи и информации в субъектах Российской Федерации входят в систему органов государственного управления и осуществляют на соответствующей территории руководство в области организации и обеспечения правительственной связи, иных видов специальной связи и информации, сбора и передачи информации экономического характера в интересах государственных органов; в пределах своей компетенции они непосредственно проводят работу по основным направлениям деятельности федеральных органов правительственной связи и информации, организуют, координируют и контролируют деятельность подчиненных им подразделений и несут ответственность за обеспечение государственных органов специальными

видами связи и информации.
Согласно Указу Президента РФ от 24 декабря 1993 г. NB 2288 часть вторая статьи 7 настоящего Указа не подлежит применению органами государственной власти, органами местного самоуправления и их должностными лицами в части согласования положений с комитетом Верховного Совета Российской Федерации и высшими должностными лицами субъектов Российской Федерации.
Организация деятельности органов правительственной связи и информации в субъектах Российской Федерации определяется соответствующими положениями, утверждаемыми генеральным директором Федерального агентства по согласованию с высшими должностными лицами субъектов Российской Федерации.

**Статья 8. Войска Федерального агентства правительственной связи и информации при Президенте Российской Федерации**

Войска Федерального агентства правительственной связи и информации при Президенте Российской Федерации включают в себя войска правительственной связи, части радиоразведки и инженерно-строительные части, которые создаются, содержатся и используются, в том числе за пределами Российской Федерации, в соответствии с законодательством Российской Федерации.
Командующим войсками Федерального агентства является генеральный директор.

**Статья 9. Взаимодействие федеральных органов правительственной связи и информации с иными государственными органами и организациями**

Федеральные органы правительственной связи и информации решают поставленные перед ними задачи во взаимодействии с Министерством безопасности Российской Федерации, Министерством обороны Российской Федерации, Министерством иностранных дел Российской Федерации, Министерством внутренних дел Российской Федерации, Министерством связи Российской Федерации, Службой внешней разведки Российской Федерации, Главным управлением охраны Российской Федерации, Государственной технической комиссией при Президенте Российской Федерации, с иными государственными органами и организациями.
Государственные органы обязаны оказывать федеральным органам правительственной связи и информации содействие в их деятельности по обеспечению функционирования правительственной связи, иных видов специальной связи, по сохранности государственных секретов и специальному информационному обеспечению высших органов государственной власти Российской Федерации, центральных органов федеральной исполнительной власти.

**Раздел III. Обязанности и права федеральных органов правительственной связи и информации**

**Статья 10. Обязанности федеральных органов правительственной связи я информации**

Федеральные органы правительственной связи и информации обязаны:
а) обеспечивать правительственной связью в местах постоянного или временного пребывания Президента Российской Федерации, Председателя Верховного Совета Российской Федерации, Председателя Правительства Российской Федерации, Председателя Конституционного Суда Российской Федерации, Председателя Верховного Суда Российской Федерации и Председателя Высшего арбитражного суда Российской Федерации;
б) участвовать в пределах своей компетенции с Главным управлением охраны Российской Федерации в организации и обеспечении президентской связи, соблюдая при этом ее единство, надежность, безопасность и оперативность;
в) обеспечивать правительственной связью, иными видами специальной связи государственные органы, высшее военное руководство и командования

объединений Вооруженных Сил Российской Федерации, а также организации, предприятия, банки и иные учреждения. Принципы организации и порядок использования правительственной связи определяются Положением о правительственной связи Российской Федерации, утверждаемым Президентом Российской Федерации по согласованию с руководителями высших органов законодательной и судебной власти Российской Федерации;

г) осуществлять разведывательную деятельность в сфере шифрованной, засекреченной и иных видов специальной связи;

д) обеспечивать высшие органы государственной власти Российской Федерации, центральные органы федеральной исполнительной власти, Совет безопасности Российской Федерации специальной информацией, необходимой им для принятия решений в области безопасности, обороны, экономики, науки и техники, международных отношений, экологии, а также мобилизационной готовности;

е) осуществлять координацию деятельности по вопросам безопасности (в том числе на этапах создания, развития и эксплуатации) информационно-аналитических сетей, комплексов технических средств баз данных высших органов государственной власти и Совета безопасности Российской Федерации;

ж) обеспечивать безопасность правительственной связи Российской Федерации;

з) координировать на безвозмездной основе в интересах обеспечения сохранения государственной и иной охраняемой законом тайны деятельность организаций, предприятий, учреждений независимо от их ведомственной принадлежности и форм собственности в области разработки, производства и поставки шифровальных средств и оборудования специальной связи;

и) координировать деятельность центральных органов федеральной исполнительной власти, организаций, предприятий, банков и иных учреждений по обеспечению криптографической и инженерно-технической безопасности шифрованной связи в Российской Федерации и ее учреждениях за рубежом, снабжать их ключевыми документами;

к) участвовать в обеспечении защиты технических средств обработки, хранения и передачи секретной информации в учреждениях, находящихся за рубежом Российской Федерации, от ее утечки по техническим каналам;

л) обеспечивать совместно с соответствующими службами высших органов государственной власти Российской Федерации защиту особо важных помещений этих органов и находящихся в них технических средств от утечки секретной информации по техническим каналам;

м) организовывать деятельность центральных органов федеральной исполнительной власти, организаций, предприятий, банков и иных учреждений по выявлению в технических средствах электронных устройств перехвата информации и обеспечивать выявление устройств перехвата информации в особо важных помещениях и технических средствах, предназначенных для использования в органах государственной власти Российской Федерации;

н) проводить разработку и изготовление специализированных технических средств и систем для обеспечения основных направлений своей деятельности;

о) обеспечивать в своей деятельности сохранность государственной и иной специально охраняемой законом тайны;

п) обеспечивать готовность систем правительственной связи и специальной информации для работы в военное время и в чрезвычайных ситуациях; поддерживать в постоянной боевой готовности технические средства оповещения государственных органов;

р) поддерживать и обеспечивать свою мобилизационную готовность.

**Статья 11. Права федеральных органов правительственной связи и информации**

Федеральные органы правительственной связи и информации имеют право:
а) издавать нормативные акты, предписания в части организации, обеспечения функционирования и безопасности правительственной, шифрованной и иных видов специальной связи, а также безопасности информационно-аналитических сетей, комплексов технических средств баз данных высших органов государственной власти и Совета безопасности Российской Федерации;
б) доступа установленным порядком на объекты связи независимо от их ведомственной принадлежности и форм собственности, в которых проходят линии или размещены средства правительственной связи, а также выполнять на таких объектах работы, связанные с решением задач, возложенных на федеральные органы правительственной связи и информации;
в) получать на приоритетной основе в соответствующих органах, ведающих распределением и назначением радиочастот, полосы радиочастот для исключительного использования их радиосредствами правительственной связи на всей территории Российской Федерации, а также заключать договоры на аренду линий и каналов связи для обеспечения деятельности федеральных органов правительственной связи и информации в пределах выделенных средств;
г) налагать ограничения по согласованию с соответствующими органами, ведающими распределением и назначением радиочастот, на использование радиоэлектронных средств любого назначения, если они работают с нарушением требований нормативных актов и создают радиопомехи работе средств правительственной связи;
д) привлекать силы и средства связи Вооруженных Сил Российской Федерации (по согласованию с Генеральным штабом Вооруженных Сил Российской Федерации), центральных органов федеральной исполнительной власти для обеспечения специальной связью в чрезвычайных ситуациях;
е) взимать плату за пользование правительственной связью, иными видами специальной связи и распределять поступающие средства в соответствии с порядком, устанавливаемым Президентом Российской Федерации, Верховным Советом Российской Федерации и Правительством Российской Федерации; оплата услуг правительственной и иных видов специальной связи осуществляется по тарифам, согласовываемым с Министерством финансов Российской Федерации;
ж) осуществлять разведывательную деятельность в сфере шифрованной, засекреченной и иных видов специальной связи с территории Российской Федерации и за ее пределами с использованием радиоэлектронных средств и методов;
з) предоставлять информационные материалы органа внешней разведки Федерального агентства высшим органам государственной власти и Совету безопасности Российской Федерации в соответствии с порядком, утверждаемым Президентом Российской Федерации и Председателем Верховного Совета Российской Федерации;
и) требовать и получать безвозмездно от центральных органов федеральной исполнительной власти, органов государственного управления субъектов Российской Федерации, государственных организаций, предприятий, учреждений, расположенных на территории Российской Федерации, независимо от их ведомственной принадлежности информацию в соответствии с утверждаемыми перечнями показателей и регламентом их представления и поручениями Президента Российской Федерации или Председателя Правительства Российской Федерации;
к) определять порядок разработки, производства, реализации, эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации в Российской Федерации; осуществлять в пределах своей компетенции лицензирование и сертификацию этих видов деятельности, товаров и услуг;

(О мерах по соблюдению законности в области разработки производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации см. Указ Президента РФ от 3 апреля 1995 г. № 334.)

л) определять порядок и обеспечивать выдачу лицензий на экспорт и импорт шифровальных средств и нормативно-технической документации на их производство и использование; участвовать в определении порядка и обеспечении выдачи лицензий на экспорт и импорт защищенных технических средств передачи, обработки и хранения секретной информации;

(Согласно постановлению Правительства РФ от 15 апреля 1994 г. NQ 331 шифровальные средства включены в Перечень специфических товаров (работ, услуг), экспорт которых осуществляется по лицензиям и в Перечень продукции, поставки которой осуществляются потребителям, имеющим разрешение на ее применение в Российской Федерации.)

м) осуществлять лицензирование и сертификацию систем и комплексов телекоммуникаций высших органов государственной власти Российской Федерации, а также закрытых систем и комплексов телекоммуникаций органов государственной власти субъектов Российской Федерации, центральных, органов федеральной исполнительной власти, организаций, предприятий, банков и иных учреждений, расположенных на территории Российской Федерации, независимо от их ведомственной принадлежности и форм собственности;

н) осуществлять государственный контроль за состоянием криптографической и инженерно-технической безопасности шифрованной связи в органах государственной власти субъектов Российской Федерации, в центральных органах федеральной исполнительной власти, в организациях, на предприятиях, в банках и иных учреждениях независимо от их ведомственной принадлежности, а также секретно-шифровальной работы в учреждениях, находящихся за рубежом Российской Федерации (кроме секретного делопроизводства в загранаппаратах Службы внешней разведки Российской Федерации);

о) участвовать в определении порядка разработки, производства, реализации и эксплуатации технических средств обработки, хранения и передачи секретной информации, предназначенных для использования в учреждениях, находящихся за рубежом Российской Федерации;

п) участвовать в разработке нормативных актов по реализации и контролю мер защиты технических средств обработки, хранения и передачи секретной информации на местах их эксплуатации в учреждениях, находящихся за рубежом Российской Федерации;

р) определять порядок проведения работ в Российской Федерации по выявлению электронных устройств перехвата информации в технических средствах; осуществлять лицензирование деятельности по выявлению электронных устройств перехвата информации в технических средствах и помещениях государственных структур;

с) осуществлять контроль реализации рекомендаций по устранению возможных технических каналов утечки секретной информации из особо важных помещений высших органов государственной власти Российской Федерации; осуществлять контроль защищенности технических средств и объектов центральных органов федеральной исполнительной власти, защита которых входит в компетенцию Федерального агентства;

т) осуществлять контакты и сотрудничество с соответствующими службами иностранных государств по вопросам обеспечения правительственной международной связи, разведывательной деятельности в сфере шифрованной, засекреченной и иных видов специальной связи, защиты информации, организации шифрованной связи и поставок шифровальных средств;

у) проводить научно-исследовательские, опытно-конструкторские, строительные и производственные работы самостоятельно и по договорам с

организациями, предприятиями;
ф) выдавать рекомендации в соответствии с законодательством Российской Федерации по заявкам на изобретения, полезные модели и промышленные образцы в области шифровальных средств, разведывательной деятельности в сфере шифрованной, засекреченной и иных видов специальной связи, а также в пределах своей компетенции по вопросам защиты помещений и технических средств от утечки информации;
х) разрешать своим сотрудникам, являющимся военнослужащими, хранение и ношение табельного оружия и специальных средств; обеспечивать охрану объектов, зданий и сооружений силами подразделений охраны, а в необходимых случаях — с привлечением подразделений войск Федерального агентства или Вооруженных Сил Российской Федерации (по согласованию с командованием Вооруженных Сил Российской Федерации на местах), с использованием имеющихся технических средств; организацию охраны и сопровождения особо важных и совершенно секретных изделий, грузов и документов; при этом осуществлять применение сотрудниками физической силы, специальных средств, а также табельного оружия в порядке, предусмотренном общевоинскими уставами Вооруженных Сил Российской Федерации;
ц) создавать в порядке, установленном законодательством Российской Федерации, организационные структуры (подразделения и организации), необходимые для решения задач, возложенных на федеральные органы правительственной связи и информации;
ч) арендовать или приобретать необходимые для решения поставленных задач помещения, строения и другую недвижимость на территории Российской Федерации и за ее пределами;
ш) оказывать содействие на договорной основе организациям, предприятиям, учреждениям независимо от форм их собственности в разработке и реализации мер по защите коммерческой тайны с помощью технических средств, если это не противоречит задачам и принципам деятельности федеральных органов правительственной связи и информации.

**Раздел IV. Силы и средства федеральных органов правительственной связи и информации**

**Статья 12. Сотрудники федеральных органов правительственной связи и информации**

1. Сотрудниками федеральных органов правительственной связи и информации являются военнослужащие, служащие и рабочие.
Общая численность сотрудников федеральных органов правительственной связи и информации определяется Президентом Российской Федерации.
2. На службу в федеральные органы правительственной связи и информации принимаются граждане Российской Федерации, способные по своим личным, моральным, деловым и профессиональным качествам, образованию и состоянию здоровья выполнять задачи, поставленные перед этими органами.
Комплектование войск военнослужащими осуществляется в добровольном порядке — по контрактам, а также на основе призыва граждан Российской Федерации на военную службу в порядке, установленном законодательством Российской Федерации.
3. Военнослужащие федеральных органов правительственной связи и информации проходят военную службу на основании законодательства Российской Федерации, воинских уставов, других нормативных актов и положений, регламентирующих военную службу. Они и члены их семей пользуются правами и льготами, предоставленными военнослужащим Вооруженных Сил Российской Федерации и членам их семей.
Военнослужащие федеральных органов правительственной связи и информации, уволенные в запас с военной службы, зачисляются в соответствии с законодательством Российской Федерации в запас Министерства безопасности Российской Федерации или Министерства обороны

Российской Федерации.
4. Трудовая деятельность служащих и рабочих федеральных органов правительственной связи и информации регламентируется законодательством Российской Федерации о труде и о государственной службе, а также издаваемыми в соответствии с ними нормативными актами Федерального агентства.
5. Обязанности и права конкретных категорий сотрудников федеральных органов правительственной связи и информации определяются настоящим Законом, другими законами Российской Федерации, указами Президента Российской Федерации и нормативными актами Правительства Российской Федерации, а также издаваемыми в соответствии с ними нормативными актами Федерального агентства.
6. Сотрудники федеральных органов правительственной связи и информации могут быть награждены нагрудным знаком «Почетный сотрудник федеральных органов правительственной связи и информации». Основания и порядок представления к награждению указанным нагрудным знаком, определяются генеральным директором Федерального агентства.

**Статья 13. Правовое положение сотрудников федеральных органов правительственной связи и информации**

1. Сотрудники, федеральных органов правительственной связи и информации при исполнении служебных обязанностей находятся под защитой государства. Никто, кроме должностных лиц, прямо уполномоченных на то законом, не вправе вмешиваться в их служебную деятельность.
Требования сотрудников федеральных органов правительственной связи и информации, предъявляемые в пределах их компетенции при исполнении служебных обязанностей, являются обязательными для исполнения государственными органами, организациями, предприятиями, учреждениями Российской Федерации.
2. Защита от посягательств на жизнь и здоровье, честь и достоинство, а также на имущество сотрудника федерального органа правительственной связи и информации и членов его семьи при исполнении им служебных обязанностей осуществляется в соответствии с законодательством Российской Федерации.
3. Не допускаются привод, административное задержание сотрудника федерального органа правительственной связи и информации, а также личный досмотр и досмотр его вещей, личного и используемого транспорта при исполнении им служебных обязанностей без участия представителя этого органа либо без санкции прокурора.
4. При получении от кого бы то ни было приказа или указания, противоречащего законодательству Российской Федерации, сотрудник федерального органа правительственной связи и информации вне зависимости от его служебного положения обязан выполнять только требования законодательства.
5. Сотрудникам федеральных органов правительственной связи и информации запрещаются организация забастовок и участие в их проведении.
6. Военнослужащие федеральных органов правительственной связи и информации не вправе заниматься внеслужебной оплачиваемой деятельностью, кроме преподавательской, научной и творческой.
7. Служащие и рабочие федеральных органов правительственной связи и информации имеют право на создание профессиональных союзов.
8. Законодательные акты Российской Федерации по вопросам труда, оплаты труда, пенсионного обеспечения, социальной и правовой защиты граждан применяются в отношении служащих и рабочих федеральных органов правительственной связи и информации независимо от объявления об их введении в действие приказами руководства Федерального агентства.
См. Закон РФ от 12 февраля 1993 г. NQ 4468-1 «О пенсионном обеспечении лиц, проходивших военную службу, службу в органах внутренних дел, и их

семей».
Согласно постановлению СМ РФ от 22 сентября 1993 г. № 941 военная служба в федеральных органах правительственной связи и информации засчитывается в выслугу лет для назначения пенсий после увольнения со службы.
9. Сотрудники федеральных органов правительственной связи и информации, исполняющие обязанности, связанные с требованиями повышенной секретности и особыми условиями службами (работы), пользуются дополнительными льготами по денежному содержанию (заработной плате), исчислению выслуги лет (трудового стажа) и социальному обеспечению, устанавливаемыми высшими органами государственной власти Российской Федерации.

**Статья 14. Ответственность сотрудников федеральных органов правительственной связи и информации**

1. Сотрудники федеральных органов правительственной связи и информации при осуществлении своих должностных функций действуют в соответствии с обязанностями и правами, установленными законодательством Российской Федерации. Действия сотрудников обжалуются в федеральные органы правительственной связи и информации и в суд.
2. Отключение правительственной и иных видов специальной связи у Президента Российской Федерации, Председателя Верховного Совета Российской Федерации и Председателя Конституционного Суда Российской Федерации без их ведома, неправомерное прекращение предоставления услуг правительственной и иных видов специальной связи другим пользователям без ведома лиц, наделенных правом разрешать предоставление этих услуг, преследуются по закону.
3. За противоправные деяния сотрудники несут предусмотренную законодательством дисциплинарную, административную, уголовную, гражданско-правовую ответственность.

**Статья 15. Социальная защита сотрудников федеральных органов правительственной связи и информации**

1. Государство гарантирует социальную защиту сотрудников федеральных органов правительственной связи и информации, а также жилищное и пенсионное обеспечение в соответствии с законодательством Российской Федерации.
2. Сотрудники федеральных органов правительственной связи и информации, направляемые в служебные командировки, пользуются правом бронирования и получения вне очереди мест в гостинице и приобретения проездных документов на все виды транспорта в порядке, определяемом Правительством Российской Федерации.
См. Правила предоставления гостиничных услуг в Российской Федерации, утвержденные постановлением Правительства РФ от 25 апреля 1997 г. NQ 490.
3. Президент Российской Федерации, Верховный Совет Российской Федерации и Правительство Российской Федерации могут устанавливать или распространять на сотрудников федеральных органов правительственной связи и информации и иные не предусмотренные настоящим Законом льготы и меры социальной защиты.

**Статья 16. Специальные технические средства федеральных органов правительственной связи и информации**

Федеральные органы правительственной связи и информации в пределах своей компетенции разрабатывают, создают и используют специальные технические средства, а также обеспечивают их сохранность с целью реализации поставленных перед ними задач и возложенных на них обязанностей.
Порядок использования специальных технических средств устанавливается нормативными актами Федерального агентства по согласованию с Верховным

Советом Российской Федерации.
О мерах по упорядочению разработки, производства, реализации, приобретения в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы, а также использования специальных технических средств, предназначенных для негласного получения информации см. Указ Президента РФ от 9 января 1996 г. № 21.

**Статья 17. Финансовое и материально-техническое обеспечение федеральных органов правительственной связи и информации**

1. Финансовое и материально-техническое обеспечение федеральных органов правительственной связи и информации осуществляется за счет средств республиканского бюджета Российской Федерации.
2. Годовой бюджет федеральных органов правительственной связи и информации утверждается Верховным Советом Российской Федерации по представлению Президента Российской Федерации одновременно с республиканским бюджетом Российской Федерации.
Порядок материально-технического обеспечения федеральных органов правительственной связи и информации устанавливается Президентом Российской Федерации по представлению генерального директора Федерального агентства.
3. Правительство Российской Федерации определяет перечень предприятий, учреждений и организаций независимо от их ведомственной принадлежности и организационно-правовых форм, которые на приоритетной основе в рамках государственного заказа осуществляют разработку, производство и поставку вооружения, военной и специальной техники, продукции производственно-технического назначения для федеральных органов правительственной связи и информации.
4. Финансовое, тыловое и техническое обеспечение войск (за исключением средств связи) осуществляется довольствующими органами Министерства обороны Российской Федерации. Расчеты за обеспечение войск всеми видами довольствия в мирное время осуществляются централизованно за счет средств Федерального агентства. В военное время такое обеспечение производится в соответствии с законодательством Российской федерации о военном положении.
5. Земельные участки, предприятия, здания, сооружения, помещения, оборудование и другое имущество, а также иные объекты, находящиеся в ведении или в оперативном управлении федеральных органов правительственной связи и информации, являются исключительно федеральной собственностью.
Распоряжением Госкомимущества РФ от 11 апреля 1997 г. № 257-р ФАПСИ разрешена реализация высвобождаемого имущества через Специализированное государственное хозрасчетное предприятие при Минобороны РФ.

**Статья 18. Защита информации федеральных органов правительственной связи и информации**

1. Лица, оформляемые на службу (работу) в федеральные органы правительственной связи и информации, которые по роду своей деятельности будут иметь доступ к сведениям, составляющим государственную или иную специально охраняемую законом тайну, проходят процедуру оформления допуска к указанным сведениям и несут ответственность в соответствии с законодательством Российской Федерации за нарушение порядка сохранения этих сведений.
Сотрудникам федеральных органов правительственной связи и информации после прекращения их службы (работы) в этих органах запрещается использовать, разглашать, распространять, передавать ставшие известными им сведения и приобретенные знания о государственных шифрах, методах разведывательной деятельности в сфере шифрованной, засекреченной и иных видов специальной связи, содержащие государственную или иную специально охраняемую законом тайну, без разрешения Федерального агентства.

2. Все лица, получившие доступ к государственным шифрам, а также к сведениям о деятельности федеральных органов правительственной связи и информации, составляющим государственную или иную специально охраняемую законом тайну, несут ответственность за нарушение порядка их сохранения в соответствии с законодательством Российской Федерации.

3. Документальные материалы, касающиеся деятельности федеральных органов правительственной связи и информации, хранятся в архивах этих органов. Материалы архивов федеральных органов правительственной связи и информации, представляющие историческую и научную ценность и рассекреченные в соответствии с законодательством Российской Федерации, передаются в Государственную архивную службу Российской Федерации.

**Статья 19. Криптографический резерв Федерального агентства правительственной связи и информации при Президенте Российской Федерации**

Для поддержания на должном уровне криптографического потенциала Российской Федерации генеральный директор Федерального агентства имеет право создавать криптографический резерв из числа ушедших в запас или в отставку высококвалифицированных криптографов, а также из числа других специалистов по своему усмотрению. Зачисляемые в криптографический резерв дают согласие на возвращение, в случае необходимости, на работу и выполнение обязанностей, определяемых генеральным директором Федерального агентства.

Генеральный директор Федерального агентства имеет право в пределах выделенных ассигнований создавать специальный фонд и определять порядок его использования для привлечения специалистов в криптографический резерв.

**Раздел V. Контроль и надзор за деятельностью федеральных органов правительственной связи и информации**

**Статья 20. Президентский контроль**

Президент Российской Федерации осуществляет контроль за ходом выполнения основных задач, возложенных на Федеральное агентство, утверждает программы развития федеральных органов правительственной связи и информации и санкционирует проведение мероприятий этих органов, затрагивающих жизненно важные интересы Российской Федерации.

**Статья 21. Парламентский контроль**

Контроль Верховного Совета Российской Федерации за деятельностью федеральных органов правительственной связи и информации осуществляется в форме заслушивания отчетов генерального директора Федерального агентства, а также сообщений должностных лиц федеральных органов правительственной связи и информации в Верховном Совете Российской Федерации.

Контроль Верховного Совета Российской Федерации за деятельностью федеральных органов правительственной связи и информации осуществляет Комитет Верховного Совета Российской Федерации по вопросам обороны и безопасности.

Народные депутаты Российской Федерации могут получать охраняемые законом сведения о деятельности федеральных органов правительственной связи и информации в порядке, определяемом законами Российской Федерации.

**Статья 22. Прокурорский надзор**

Надзор за исполнением законов Российской Федерации федеральными органами правительственной связи и информации осуществляют Генеральный прокурор Российской Федерации и подчиненные ему прокуроры.

**Статья 23. Связь федеральных органов правительственной связи и информации с общественностью**

1. Федеральные органы правительственной связи и информации осуществляют информирование общественности о своей деятельности через создаваемые в

составе этих органов соответствующие службы.
2. Представляемые средствам массовой информации материалы о деятельности федеральных органов правительственной связи и информации не должны содержать сведений, отнесенных в соответствии с законодательством Российской Федерации к государственной и иной специально охраняемой законом тайне.
3. Сотрудники федеральных органов правительственной связи и информации выступают в средствах массовой информации по вопросам деятельности этих органов только с санкции их руководителей. Материалы о деятельности федеральных органов правительственной связи и информации, подготовленные к опубликованию бывшими сотрудниками этих органов или при их содействии, представляются на рассмотрение в соответствующие федеральные органы правительственной связи и информации для вынесения мотивированного решения о возможности или невозможности их публикации.

**Москва, Дом Советов России**
**19 февраля 1993 г.**
**Президент Российской Федерация Б. Ельцин**

**«ОБ ОРГАНАХ ФЕДЕРАЛЬНОЙ СЛУЖБЫ БЕЗОПАСНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ»**

**Федеральный закон от 3 апреля 1995 г. № 40-ФЗ Принят Государственной Думой 22 февраля 1995 г.**

Настоящий Федеральный закон определяет назначение, правовые основы, принципы, направления деятельности, полномочия, силы и средства органов Федеральной службы безопасности, а также порядок контроля и надзора за их деятельностью.

**Глава I. Общие положения**

**Статья 1. Органы Федеральной службы безопасности и их назначение**

Органы Федеральной службы безопасности являются составной частью сил обеспечения безопасности Российской Федерации и в пределах предоставленных им полномочий обеспечивают безопасность личности, общества и государства.
Руководство деятельностью органов Федеральной службы безопасности осуществляют Президент Российской Федерации и Правительство Российской Федерации.

**Статья 2. Система органов Федеральной службы безопасности**

Органы Федеральной службы безопасности представляют собой единую централизованную систему, в которую входят:
>• Федеральная служба безопасности Российской Федерации;
>• управления (отделы) Федеральной службы безопасности Российской Федерации по отдельным регионам и субъектам Российской Федерации (территориальные органы безопасности);
>• управления (отделы) Федеральной службы безопасности Российской Федерации в Вооруженных Силах Российской Федерации, войсках и иных воинских формированиях, а также в их органах управления (органы безопасности в войсках).
Территориальные органы безопасности и органы безопасности в войсках находятся в прямом подчинении Федеральной службе безопасности Российской Федерации.
Органы Федеральной службы безопасности в своем подчинении имеют предприятия, учебные заведения, научно-исследовательские, экспертные и военно-медицинские учреждения и подразделения, военно-строительные подразделения, центры специальной подготовки, а также подразделения специального назначения.
Создание органов Федеральной службы безопасности, не предусмотренных настоящим Федеральным законом, не допускается.
В органах Федеральной службы безопасности запрещаются создание организационных структур и деятельность политических партий, массовых общественных движений, преследующих политические цели а также ведение

политической агитации и предвыборных кампаний.

**Статья 3. Федеральная служба безопасности Российской Федерации**

Федеральная служба безопасности Российской Федерации является Федеральным органом исполнительной власти.

Федеральная служба безопасности Российской Федерации создает территориальные органы безопасности и органы безопасности в войсках, осуществляет руководство ими и организует их деятельность, издает в пределах своих полномочий нормативные акты и непосредственно реализует основные направления деятельности органов Федеральной службы безопасности.

Структура и организация деятельности Федеральной службы безопасности Российской Федерации определяются положением о Федеральной службе безопасности Российской Федерации, утверждаемым Президентом Российской Федерации.

Положение о Федеральной службе безопасности Российской Федерации и ее структура утверждены Указом Президента РФ от 6 июля 1998 г. № 806.

Федеральную службу безопасности Российской Федерации возглавляет Директор Федеральной службы безопасности Российской Федерации на правах Федерального министра. Должности Директора Федеральной службы безопасности Российской Федерации соответствует воинское звание генерал армии.

**Статья 4. Правовая основа деятельности органов Федеральной службы безопасности**

Правовую основу деятельности органов Федеральной службы безопасности составляют Конституция Российской Федерации, настоящий Федеральный закон, другие федеральные законы и иные нормативные правовые акты федеральных органов государственной власти.

Деятельность органов Федеральной службы безопасности осуществляется также в соответствии с международными договорами Российской Федерации.

**Статья 5. Принципы деятельности органов Федеральной службы безопасности**

Деятельность органов Федеральной службы безопасности осуществляется на основе принципов:

>• законности;

>• уважения и соблюдения прав и свобод человека и гражданина;

>• гуманизма;

**>•** единства системы органов Федеральной службы безопасности и централизации управления ими;

>• конспирации, сочетания гласных и негласных методов и средств деятельности.

**Статья 6. Соблюдение прав и свобод человека и гражданина в деятельности органов Федеральной службы безопасности**

Государство гарантирует соблюдение прав и свобод человека и гражданина при осуществлении органами Федеральной службы безопасности своей деятельности. Не допускается ограничение прав и свобод человека и гражданина, за исключением случаев, предусмотренных федеральными конституционными законами и федеральными законами.

Лицо, полагающее, что органами Федеральной службы безопасности либо их должностными лицами нарушены его права и свободы, вправе обжаловать действия указанных органов и должностных лиц в вышестоящий орган Федеральной службы безопасности, прокуратуру или суд.

Государственные органы, предприятия, учреждения и организации независимо от форм собственности, а также общественные Объединения и граждане имеют право в соответствии с законодательством Российской Федерации получать разъяснения и информацию от органов Федеральной службы безопасности в случае ограничения своих прав и свобод.

Государственные органы, предприятия, учреждения и организации независимо от форм собственности, а также общественные объединения и

граждане вправе требовать от органов Федеральной службы безопасности возмещения морального и материального ущерба, причиненного действиями должностных лиц органов Федеральной службы безопасности при исполнении ими служебных обязанностей.

О порядке возмещения ущерба, причиненного гражданину незаконными действиями органов ФСБ при производстве дознания и предварительном следствии, см. Указ Президиума ВС СССР от 18 мая 1981 г. № 4892-X и инструкцию, утвержденную Минюстом СССР, Прокуратурой СССР и Минфином СССР по согласованию с Верховным Судом СССР, МВД СССР и КГБ СССР 2 марта 1982 г.

Полученные в процессе деятельности органов Федеральной службы безопасности сведения о частной жизни, затрагивающие честь и достоинство гражданина или способные повредить его законным интересам, не могут сообщаться органами Федеральной службы безопасности кому бы то ни было без добровольного согласия гражданина, за исключением случаев, предусмотренных федеральными законами.

В случае нарушения сотрудниками органов Федеральной службы безопасности прав и свобод человека и гражданина руководитель соответствующего органа Федеральной службы безопасности, прокурор или судья обязаны принять меры по восстановлению этих прав и свобод, возмещению причиненного ущерба и привлечению виновных к ответственности, предусмотренной законодательством Российской Федерации.

Должностные лица органов Федеральной службы безопасности, допустившие злоупотребление властью или превышение служебных полномочий, несут ответственность, предусмотренную законодательством Российской Федерации.

**Статья 7. Защита сведений об органах Федеральной службы безопасности**

Граждане Российской Федерации, принимаемые на военную службу (работу) в органы Федеральной службы безопасности, а также допускаемые к сведениям об органах Федеральной службы безопасности, проходят процедуру оформления допуска к сведениям, составляющим государственную тайну, если иной порядок не предусмотрен законодательством Российской Федерации. Такая процедура включает принятие обязательства о неразглашении этих сведений.

Граждане Российской Федерации, допущенные к сведениям об органах Федеральной службы безопасности, составляющим государственную тайну, несут за их разглашение ответственность, предусмотренную законодательством Российской Федерации.

Документы и материалы, содержащие сведения о кадровом составе органов Федеральной службы безопасности, лицах, оказывающих или оказывавших им содействие на конфиденциальной основе, а также об организации, о тактике, методах и средствах осуществления органами Федеральной службы безопасности контрразведывательной, разведывательной и оперативно-розыскной деятельности, подлежат хранению в архивах органов Федеральной службы безопасности.

Материалы архивов органов Федеральной службы безопасности, представляющие историческую и научную ценность, рассекречиваемые в, соответствии с законодательством Российской Федерации, передаются на хранение в архивы Государственной архивной службы России в порядке, установленном законодательством Российской Федерации.

**Глава II. Основные направления деятельности органов Федеральной службы безопасности**

**Статья 8. Деятельность органов Федеральной службы безопасности**

Деятельность органов Федеральной службы безопасности осуществляется по следующим основным направлениям:

>• контрразведывательная деятельность;

>• борьба с преступностью.

Разведывательная деятельность, иные направления деятельности органов Федеральной службы безопасности определяются настоящим Федеральным законом и другими федеральными законами.
Для документирования деятельности органов Федеральной службы безопасности и ее результатов могут использоваться информационные системы, видео- и аудиозапись, кино- и фотосъемка, другие технические и иные средства.
Деятельность органов Федеральной службы безопасности, применяемые ими методы и средства не должны причинять ущерб жизни и здоровью людей и наносить вред окружающей среде.

**Статья 9. Контрразведывательная деятельность**

Контрразведывательная деятельность — деятельность органов Федеральной службы безопасности в пределах своих полномочий по выявлению, предупреждению, пресечению разведывательной и иной деятельности специальных служб и организаций иностранных государств, а также отдельных лиц, направленной на нанесение ущерба безопасности Российской Федерации.
Основаниями для осуществления органами Федеральной службы безопасности контрразведывательной деятельности являются:
а) наличие данных о признаках разведывательной и иной деятельности специальных служб и организаций иностранных государств, а также отдельных лиц, направленной на нанесение ущерба безопасности Российской Федерации;
б) необходимость обеспечения защиты сведений, составляющих государственную тайну;
в) необходимость изучения (проверки) лиц, оказывающих или оказывавших содействие органам Федеральной службы безопасности на конфиденциальной основе;
г) необходимость обеспечения собственной безопасности. Перечень оснований для осуществления контрразведывательной деятельности является исчерпывающим и может быть изменен или дополнен только федеральными законами. В процессе контрразведывательной деятельности органы Федеральной службы безопасности могут использовать гласные и негласные методы и средства, особый характер которых определяется условиями этой деятельности.
Порядок использования негласных методов и средств при осуществлении контрразведывательной деятельности определяется нормативными актами Федеральной службы безопасности Российской Федерации.
Осуществление контрразведывательной деятельности, затрагивающей тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений граждан, допускается только на основании судебного решения в порядке, предусмотренном законодательством Российской Федерации.
Осуществление контрразведывательной деятельности, затрагивающей неприкосновенность жилища граждан, допускается только в случаях, установленных федеральным законом, или на основании судебного решения.
Для получения судебного решения на право осуществления контрразведывательной деятельности в случаях, предусмотренных частями шестой и седьмой настоящей статьи, органы Федеральной службы безопасности по требованию суда представляют служебные документы, касающиеся оснований для осуществления контрразведывательной деятельности (за исключением оперативно-служебных документов, содержащих сведения о лицах, оказывающих или оказывавших содействие органам Федеральной службы безопасности на конфиденциальной основе, а также об организации, о тактике, методах и средствах осуществления контрразведывательной деятельности).
Судебное решение на право осуществления контрразведывательной деятельности и материалы, послужившие основанием для его принятия,

хранятся в органах Федеральной службы безопасности в порядке, установленном настоящим Федеральным законом.
Постановление органа Федеральной службы безопасности об осуществлении контрразведывательной деятельности и судебное решение по нему, а также материалы оперативных дел представляются в органы прокуратуры только в случаях проведения в порядке надзора проверок по поступившим в прокуратуру материалам, информации, обращениям граждан, свидетельствующим о нарушении органами Федеральной службы безопасности законодательства Российской Федерации.
Сведения об организации, о тактике, методах и средствах осуществления контрразведывательной деятельности составляют государственную тайну.

**Статья 10. Борьба с преступностью**

Органы Федеральной службы безопасности в соответствии с законодательством Российской Федерации осуществляют оперативно-розыскные мероприятия по выявлению, предупреждению, пресечению и раскрытию шпионажа, террористической деятельности, организованной преступности, коррупции, незаконного оборота оружия и наркотических средств, контрабанды и других преступлений, дознание и предварительное следствие по которым отнесены законом к их ведению, а также по выявлению, предупреждению, пресечению и раскрытию деятельности незаконных вооруженных формирований, преступных групп, отдельных лиц и общественных объединений, ставящих своей целью насильственное изменение конституционного строя Российской Федерации.
На органы Федеральной службы безопасности федеральными законами и иными нормативными правовыми актами федеральных органов государственной власти могут возлагаться и другие задачи в сфере борьбы с преступностью.
Деятельность органов Федеральной службы безопасности в сфере борьбы с преступностью осуществляется в соответствии с Законом Российской Федерации «Об оперативно-розыскной деятельности в Российской Федерации», уголовным и уголовно-процессуальным законодательством Российской Федерации, а также настоящим Федеральным законом.

**Статья 11. Разведывательная деятельность**

Разведывательная деятельность осуществляется органами Федеральной службы безопасности в пределах своих полномочий и во взаимодействии с органами внешней разведки Российской Федерации в целях получения информации об угрозах безопасности Российской Федерации.
Порядок и условия взаимодействия органов Федеральной службы безопасности и органов внешней разведки Российской Федерации устанавливаются на основании соответствующих соглашений между ними или совместных нормативных актов.
Порядок проведения разведывательных мероприятий, а также порядок использования негласных методов и средств при осуществлении разведывательной деятельности определяются нормативными актами Федеральной службы безопасности Российской Федерации.
Сведения об организации, о тактике, методах и средствах осуществления разведывательной деятельности составляют государственную тайну.

**Глава III. Полномочия органов Федеральной службы безопасности**

**Статья 12. Обязанности органов Федеральной службы безопасности**

Органы Федеральной службы безопасности обязаны:
а) информировать Президента Российской Федерации, Председателя Правительства Российской Федерации и по их поручениям федеральные органы государственной власти, а также органы государственной власти субъектов Российской Федерации об угрозах безопасности Российской Федерации;
б) выявлять, предупреждать, пресекать разведывательную и иную деятельность специальных служб и организаций иностранных государств, а

также отдельных лиц, направленную на нанесение ущерба безопасности Российской Федерации;
в) добывать разведывательную информацию в интересах обеспечения безопасности Российской Федерации, повышения ее экономического, научно-технического и оборонного потенциала;
г) выявлять, предупреждать и пресекать преступления, дознание и предварительное следствие по которым отнесены законодательством Российской Федерации к ведению органов Федеральной службы безопасности; осуществлять розыск лиц, совершивших указанные преступления или подозреваемых в их совершении;
д) выявлять, предупреждать и пресекать акты терроризма;
е) разрабатывать и осуществлять во взаимодействии с другими государственными органами меры по борьбе с коррупцией, незаконным оборотом оружия и наркотических средств, контрабандой, деятельностью незаконных вооруженных формирований, преступных групп, отдельных лиц и общественных объединений, ставящих своей целью насильственное изменение конституционного строя Российской Федерации;
ж) обеспечивать в пределах своих полномочий безопасность в Вооруженных Силах Российской Федерации, Пограничных войсках Российской Федерации, внутренних войсках Министерства внутренних дел Российской Федерации, Войсках Федерального агентства правительственной связи и информации при Президенте Российской Федерации, Железнодорожных войсках Российской Федерации, Войсках гражданской обороны Российской Федерации, иных воинских формированиях и в их органах управления, а также в органах внутренних дел, федеральных органах налоговой полиции, Федеральных органах правительственной связи и информации, таможенных органах Российской Федерации;
з) обеспечивать в пределах своих полномочий безопасность объектов оборонного комплекса, атомной энергетики, транспорта и связи, жизнеобеспечения крупных городов и промышленных центров, других стратегических объектов, а также безопасность в сфере космических исследований, приоритетных научных разработок;
и) обеспечивать в пределах своих полномочий безопасность федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации;
к) участвовать в разработке и реализации мер по защите сведений, составляющих государственную тайну; осуществлять контроль за обеспечением сохранности сведений, составляющих государственную тайну, в государственных органах, воинских формированиях, на предприятиях, в учреждениях и организациях независимо от форм собственности; в установленном порядке осуществлять меры, связанные с допуском граждан к сведениям, составляющим государственную тайну;
л) проводить во взаимодействии со Службой внешней разведки Российской Федерации мероприятия по обеспечению безопасности учреждений и граждан Российской Федерации за ее пределами;
м) осуществлять в пределах своих полномочий и во взаимодействии с Пограничными войсками Российской Федерации меры по обеспечению охраны Государственной границы Российской Федерации;
н) обеспечивать во взаимодействии с органами внутренних дел безопасность представительств иностранных государств на территории Российской Федерации;
о) участвовать в пределах своих полномочий совместно с другими государственными органами в обеспечении безопасности проводимых на территории Российской Федерации общественно-политических, религиозных и иных массовых мероприятий;
п) осуществлять регистрацию и централизованный учет радиоданных и радиоизлучений передающих радиоэлектронных средств; выявлять на

территории Российской Федерации радиоизлучения передающих радиоэлектронных средств, работа которых представляет угрозу безопасности Российской Федерации, а также радиоизлучения передающих радиоэлектронных средств, используемых в противоправных целях;
р) участвовать в соответствии с законодательством Российской Федерации в решении вопросов, касающихся приема в гражданство Российской Федерации и выхода из него, въезда на территорию Российской Федерации и выезда за ее пределы граждан Российской Федерации, иностранных граждан и лиц без гражданства, а также режима пребывания иностранных граждан и лиц без гражданства на территории Российской Федерации;
с) поддерживать мобилизационную готовность органов Федеральной службы безопасности;
т) осуществлять подготовку кадров для органов Федеральной службы безопасности, их переподготовку и повышение их квалификации.
Об участии органов ФСБ в обеспечении безопасности объектов государственной охраны и защиты охраняемых объектов см. Федеральный закон от 27 мая 1996 г. № 57-ФЗ.

**Статья 13. Права органов Федеральной службы безопасности**

Органы Федеральной службы безопасности имеют право:
а) устанавливать на конфиденциальной основе отношения сотрудничества с лицами, давшими на то согласие;
б) осуществлять оперативно-розыскные мероприятия по выявлению, предупреждению, пресечению и раскрытию шпионажа, террористической деятельности, организованной преступности, коррупции, незаконного оборота оружия и наркотических средств, контрабанды и других преступлений, дознание и предварительное следствие по которым отнесены законодательством Российской Федерации к ведению органов Федеральной службы безопасности, а также по выявлению, предупреждению, пресечению и раскрытию деятельности незаконных вооруженных формирований, преступных групп, отдельных лиц и общественных объединений, ставящих своей целью насильственное изменение конституционного строя Российской Федерации;
в) осуществлять проникновение в специальные службы и организации иностранных государств, проводящие разведывательную и иную деятельность, направленную на нанесение ущерба безопасности Российской Федерации, а также в преступные группы;
г) осуществлять дознание и предварительное следствие по делам о преступлениях, отнесенных законодательством Российской Федерации к ведению органов Федеральной службы безопасности; иметь и использовать в соответствии с законодательством Российской Федерации следственные изоляторы;
О подследственности уголовных дел органам Федеральной службы безопасности см. Уголовно-процессуальный кодекс РСФСР.
д) осуществлять шифровальные работы в органах Федеральной службы безопасности, а также контроль за соблюдением режима секретности при обращении с шифрованной информацией в шифровальных подразделениях государственных органов, предприятий, учреждений и организаций независимо от форм собственности (за исключением учреждений Российской Федерации, находящихся за ее пределами);
е) использовать в служебных целях средства связи, принадлежащие государственным предприятиям, учреждениям и организациям, а в неотложных случаях — негосударственным предприятиям, учреждениям и организациям, а также общественным объединениям и гражданам Российской Федерации;
ж) использовать в случаях, не терпящих отлагательства, транспортные средства, принадлежащие предприятиям, учреждениям и организациям независимо от форм собственности или общественным объединениям (за исключением транспортных средств, которые законодательством Российской

Федерации освобождены от такого использования), для предотвращения преступлений, преследования и задержания лиц, совершивших преступления или подозреваемых в их совершении, доставления граждан, нуждающихся в срочной медицинской помощи, в лечебные учреждения, а также для проезда по месту происшествия. По требованию владельцев транспортных средств органы Федеральной службы безопасности в установленном законом порядке возмещают им расходы либо причиненный ущерб;

з) беспрепятственно входить в жилые и иные принадлежащие гражданам помещения, на принадлежащие им земельные участки, на территории и в помещения предприятий, учреждений и организаций независимо от форм собственности в случае, если имеются достаточные данные полагать, что там совершается или совершено преступление, дознание и предварительное следствие по которому отнесены законодательством Российской Федерации к ведению органов Федеральной службы безопасности, а также в случае преследования лиц, подозреваемых в совершении указанных преступлений, если промедление может поставить под угрозу жизнь и здоровье граждан. Обо всех таких случаях вхождения в жилые и иные принадлежащие гражданам помещения органы Федеральной службы безопасности уведомляют прокурора в течение двадцати четырех часов;

и) проверять у граждан и должностных лиц документы, удостоверяющие их личность, если имеются достаточные основания подозревать их в совершении преступления;

к) осуществлять административное задержание лиц, совершивших правонарушения, связанные с попытками проникновения и проникновением на специально охраняемые территории особорежимных объектов, закрытых административно-территориальных образований и иных охраняемых объектов, а также проверять у этих лиц документы, удостоверяющие их личность, получать от них объяснения, осуществлять их личный досмотр, досмотр и изъятие их вещей и документов;

л) вносить в государственные органы, администрации предприятий, учреждений и организаций независимо от форм собственности, а также в общественные объединения обязательные для исполнения представления об устранении причин и условий, способствующих реализации угроз безопасности Российской Федерации, совершению преступлений, дознание и предварительное следствие по которым отнесены законодательством Российской Федерации к ведению органов Федеральной службы безопасности;

м) получать безвозмездно от государственных органов, предприятий, учреждений и организаций независимо от форм собственности информацию, необходимую для выполнения возложенных на органы Федеральной службы безопасности обязанностей, за исключением случаев, когда федеральными законами установлен специальный порядок получения информации;

н) создавать в установленном законодательством Российской Федерации порядке предприятия, учреждения, организации и подразделения, необходимые для выполнения обязанностей, возложенных на органы Федеральной службы безопасности, и обеспечения деятельности указанных органов;

о) создавать подразделения специального назначения для выполнения обязанностей, возложенных на органы Федеральной службы безопасности;

п) проводить криминалистические и другие экспертизы и исследования;

р) осуществлять внешние сношения со специальными службами и правоохранительными органами иностранных государств, обмениваться с ними на взаимной основе оперативной информацией, специальными техническими и иными средствами в пределах полномочий органов Федеральной службы безопасности и порядке, установленном нормативными актами Федеральной службы безопасности Российской Федерации; заключать в установленном порядке и пределах своих полномочий международные договоры Российской Федерации;

с) направлять официальных представителей органов Федеральной службы безопасности в иностранные государства по согласованию со специальными службами или с правоохранительными органами этих государств в целях повышения эффективности борьбы с преступлениями международного характера;
т) осуществлять меры по обеспечению собственной безопасности, в том числе по предотвращению проникновения специальных служб и организаций иностранных государств, преступных групп и отдельных лиц с использованием технических средств к защищаемым органами Федеральной службы безопасности сведениям, составляющим государственную тайну;
у) разрешать сотрудникам органов Федеральной службы безопасности хранение и ношение табельного оружия и специальных средств;
ф) использовать в целях зашифровки личности сотрудников органов Федеральной службы безопасности, ведомственной принадлежности их подразделений, помещений и транспортных средств документы других министерств, ведомств, предприятий, учреждений и организаций;
х) проводить научные исследования проблем безопасности Российской Федерации;
ц) оказывать содействие предприятиям, учреждениям и организациям независимо от форм собственности в разработке мер по защите коммерческой тайны;
ч) осуществлять на компенсационной или безвозмездной основе подготовку кадров для специальных служб иностранных государств, служб безопасности предприятий, учреждений и организаций независимо от форм собственности, если это не противоречит принципам деятельности органов Федеральной службы безопасности.
Использование органами Федеральной службы безопасности предоставленных им прав для выполнения обязанностей, не предусмотренных федеральными законами, не допускается.

**Статья 14. Применение оружия, специальных средств и физической силы**

Сотрудникам органов Федеральной службы безопасности разрешается хранение и ношение табельного оружия и специальных средств. Они имеют право применять физическую силу, в том числе боевые приемы борьбы, а также оружие и специальные средства в случаях и порядке, предусмотренных законодательными и иными нормативными правовыми актами Российской Федерации для сотрудников милиции.
О порядке выдачи, хранения, ношения, применения (использования) сотрудниками-военнослужащими органов Федеральной службы безопасности личного табельного оружия см. Временную инструкцию, утвержденную приказом МБ РФ от 31 августа 1992 г. № 252.

**Статья 15. Взаимодействие с российскими и иностранными учреждениями**

Органы Федеральной службы безопасности осуществляют свою деятельность во взаимодействии с федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, предприятиями, учреждениями и организациями независимо от форм собственности.
Органы Федеральной службы безопасности могут использовать возможности других сил обеспечения безопасности Российской Федерации в установленном федеральными законами порядке.
Государственные органы, а также предприятия, учреждения и организации обязаны оказывать содействие органам Федеральной службы безопасности в осуществлении ими возложенных на них обязанностей.
Физические и юридические лица в Российской Федерации, предоставляющие услуги почтовой связи, электросвязи всех видов, в том числе систем телекодовой, конфиденциальной, спутниковой связи, обязаны по требованию органов Федеральной службы безопасности включать в состав аппаратных средств дополнительные оборудование и программные средства, а также

создавать другие условия, необходимые для проведения оперативно-технических мероприятий органами Федеральной службы безопасности.
В целях решения задач обеспечения безопасности Российской Федерации военнослужащие органов Федеральной службы безопасности могут быть прикомандированы к государственным органам, предприятиям, учреждениям и организациям независимо от форм собственности с согласия их руководителей в порядке, установленном Президентом Российской Федерации, с оставлением их на военной службе.
Взаимодействие органов Федеральной службы безопасности со специальными службами, с правоохранительными органами и иными организациями иностранных государств устанавливается на основании международных договоров Российской Федерации.

**Глава IV. Силы и средства органов Федеральной службы безопасности**

**Статья 16. Сотрудники органов Федеральной службы безопасности**

Органы Федеральной службы безопасности комплектуются (в том числе и на конкурсной основе) военнослужащими и гражданским персоналом.
Военнослужащие органов Федеральной службы безопасности (за исключением военнослужащих, проходящих военную службу по призыву), а также лица из числа гражданского персонала, назначенные на должности военнослужащих, являются сотрудниками органов Федеральной службы безопасности.
Сотрудником органов Федеральной службы безопасности может быть гражданин Российской Федерации, способный по своим личным и деловым качествам, возрасту, образованию и состоянию здоровья выполнять возложенные на него обязанности.
Военнослужащие органов Федеральной службы безопасности проходят военную службу в соответствии с законодательством Российской Федерации о прохождении военной службы с учетом установленных настоящим Федеральным законом особенностей, обусловленных спецификой выполняемых ими обязанностей.
Численность военнослужащих и гражданского персонала органов Федеральной службы безопасности (без учета численности работников научно-исследовательских, военно-медицинских учреждений и подразделений, персонала по эксплуатации, охране и обслуживанию служебных зданий и помещений органов Федеральной службы безопасности) устанавливается Президентом Российской Федерации. Численность военнослужащих и гражданского персонала научно-исследовательских, военно-медицинских учреждений и подразделений, персонала по эксплуатации, охране и обслуживанию служебных зданий и помещений органов Федеральной службы безопасности устанавливается Директором Федеральной службы безопасности Российской Федерации в пределах бюджетных ассигнований, выделяемых Федеральной службе безопасности Российской Федерации.
Полномочия должностных лиц органов Федеральной службы безопасности на применение поощрений и наложение дисциплинарных взысканий в отношении подчиненных им военнослужащих, а также на присвоение воинских званий, назначение и увольнение военнослужащих (за исключением военнослужащих, замещающих должности высших офицеров) устанавливаются Директором Федеральной службы безопасности Российской Федерации.
С военнослужащими органов Федеральной службы безопасности, являющимися высококвалифицированными специалистами и достигшими предельного возраста пребывания на военной службе, могут, быть заключены контракты о прохождении военной службы на период до достижения ими 65-летнего возраста в порядке, определяемом Директором Федеральной службы безопасности Российской Федерации.
Обязанности, права и льготы гражданского персонала органов Федеральной службы безопасности определяются законодательством Российской Федерации.
Сотрудники органов Федеральной службы безопасности в своей служебной

деятельности руководствуются федеральными законами и не могут быть связаны решениями политических партий, общественных движений и общественных организаций.
Сотрудникам и гражданскому персоналу органов Федеральной службы безопасности запрещается заниматься предпринимательской деятельностью, а также оказывать содействие физическим и юридическим лицам в осуществлении такой деятельности. Сотрудники органов Федеральной службы безопасности не вправе совмещать военную службу с иной оплачиваемой деятельностью, кроме занятий научной, преподавательской и иной творческой деятельностью, если она не препятствует исполнению служебных обязанностей (за исключением случаев, когда это вызвано служебной необходимостью).

**Статья 17. Правовая защита сотрудников органов Федеральной службы безопасности**

Сотрудники органов Федеральной службы безопасности при исполнении служебных обязанностей являются представителями федеральных органов государственной власти и находятся под защитой государства. Никто, кроме государственных органов и должностных лиц, уполномоченных на то федеральными законами, не вправе вмешиваться в их служебную деятельность.
Воспрепятствование исполнению сотрудником органов Федеральной службы безопасности служебных обязанностей, оскорбление, сопротивление, насилие или угроза применения насилия по отношению к нему в связи с исполнением указанным сотрудником служебных обязанностей влекут за собой ответственность, предусмотренную законодательством Российской Федерации.
Защита жизни и здоровья, чести и достоинства, а также имущества сотрудника органов Федеральной службы безопасности и членов его семьи от преступных посягательств в связи с исполнением им служебных обязанностей осуществляется в порядке, предусмотренном законодательством Российской Федерации.
При исполнении сотрудником органов Федеральной службы безопасности служебных обязанностей не допускаются его привод, задержание, личный досмотр и досмотр его вещей, а также досмотр личного и используемого им транспорта без официального представителя органов Федеральной службы безопасности или решения суда.
Сведения о сотрудниках органов Федеральной службы безопасности, выполнявших (выполняющих) специальные задания в специальных службах и организациях иностранных государств, в преступных группах, составляют государственную тайну и могут быть преданы гласности только с письменного согласия указанных сотрудников и в случаях, предусмотренных федеральными законами.

**Статья 18. Социальная защита сотрудников органов Федеральной службы безопасности**

Военнослужащим органов Федеральной службы безопасности из числа высококвалифицированных специалистов в выслугу лет для назначения пенсии и исчисления процентной надбавки за выслугу лет может засчитываться стаж их трудовой деятельности до зачисления на военную службу в порядке, определяемом Директором Федеральной службы безопасности Российской Федерации.
Время выполнения сотрудниками органов Федеральной службы безопасности специальных заданий в специальных службах и организациях иностранных государств, в преступных группах подлежит зачету в выслугу лет в льготном исчислении для назначения пенсии, присвоения воинского звания и исчисления процентной надбавки за выслугу лет в порядке, определяемом Правительством Российской Федерации.
Военнослужащим и гражданскому персоналу органов Федеральной службы

безопасности оклады по воинской должности и должностные оклады (тарифные ставки) устанавливаются с увеличением на 25 процентов за службу (работу) в органах Федеральной службы безопасности.

О надбавках и дополнительных выплатах военнослужащими и гражданскому персоналу органов Федеральной службы безопасности см. Указ Президента РФ от 6 сентября 1995 г. № 901, постановление Правительства РФ от 16 марта 1996 г. № 280.

Военнослужащим органов Федеральной службы безопасности, имеющим право на пенсию за выслугу лет и продолжающим военную службу, выплачивается ежемесячная надбавка к денежному довольствию в размере от 25 до 50 процентов размера пенсии, которая могла быть им начислена. Порядок и условия выплаты указанной надбавки определяются Директором Федеральной службы безопасности Российской Федерации.

Военнослужащие органов Федеральной службы безопасности на всей территории Российской Федерации пользуются правом бесплатного проезда на всех видах общественного транспорта городского, пригородного и местного сообщения (за исключением такси), а в сельской местности — на попутном транспорте (за исключением личного) при предъявлении служебного удостоверения.

Военнослужащие органов Федеральной службы безопасности, обеспечивающие безопасность объектов транспорта, при выполнении служебных обязанностей имеют право бесплатного проезда в поездах, на речных, морских и воздушных судах.

Сотрудникам органов Федеральной службы безопасности, использующим в служебных целях личный транспорт, выплачивается денежная компенсация в порядке и размере, устанавливаемых Правительством Российской Федерации.

Военнослужащим органов Федеральной службы безопасности телефоны по месту жительства устанавливаются в срок, не превышающий одного года со дня подачи заявления.

Оказание медицинской помощи военнослужащим и гражданскому персоналу органов Федеральной службы безопасности, членам семей военнослужащих, проходящих службу по контракту (женам, мужьям, детям в возрасте до 18 лет и лицам, находящимся на иждивении), а также детям гражданского персонала в возрасте до 18 лет в военно-медицинских учреждениях органов Федеральной службы безопасности осуществляется бесплатно.

Оказание медицинской помощи военнослужащим органов Федеральной службы безопасности, в том числе обеспечение военнослужащих лекарственными средствами, изделиями медицинского назначения, изготовление и ремонт зубных протезов (за исключением протезов из драгоценных металлов) в учреждениях здравоохранения других министерств и ведомств, осуществляется за счет средств Федеральной службы безопасности Российской Федерации. При этом средства, направляемые органами Федеральной службы безопасности учреждениям здравоохранения иной ведомственной принадлежности за оказание медицинской помощи военнослужащим, исключаются из сумм, облагаемых налогами.

Время нахождения военнослужащих органов Федеральной службы безопасности на излечении в связи с полученными ими при исполнении служебных обязанностей ранениями, контузиями или увечьями не ограничивается только при наличии неоспоримых данных о возможности восстановления способности к несению военной службы.

Права и льготы военнослужащих органов Федеральной службы безопасности и членов их семей, предусмотренные частями девятой и десятой настоящей статьи, распространяются на граждан, которые уволены с военной службы по достижении предельного возраста пребывания на военной службе, состоянию здоровья или в связи с организационно-штатными мероприятиями и общая продолжительность военной службы которых в льготном исчислении составляет двадцать и более лет, а также на членов их семей.

**Статья 19. Лица, содействующие органам Федеральной службы безопасности**

Органы Федеральной службы безопасности могут привлекать отдельных лиц с их согласия к содействию в решении возложенных на органы Федеральной службы безопасности обязанностей на гласной и негласной (конфиденциальной) основе, в том числе в качестве внештатных сотрудников. Полномочия внештатного сотрудника органов Федеральной службы безопасности определяются нормативными актами Федеральной службы безопасности Российской Федерации.

Лица, оказывающие содействие органам Федеральной службы безопасности, имеют право:

а) заключать контракт с органами Федеральной службы безопасности о конфиденциальном сотрудничестве;

б) получать от сотрудников органов Федеральной службы безопасности разъяснения своих задач, обязанностей и прав;

в) использовать в целях конспирации документы, зашифровывающие личность;

г) получать вознаграждение;

д) получать компенсацию за ущерб, причиненный их здоровью либо имуществу в процессе оказания содействия органам Федеральной службы безопасности.

Лица, оказывающие содействие органам Федеральной службы безопасности, обязаны:

а) соблюдать условия заключаемого с органами Федеральной службы безопасности контракта или договоренности о сотрудничестве;

б) выполнять поручения органов Федеральной службы безопасности, направленные на осуществление возложенных на них обязанностей;

в) не допускать умышленного предоставления необъективной, неполной, ложной или клеветнической информации;

г) не разглашать сведения, составляющие государственную тайну, и иные сведения, ставшие им известными в процессе оказания содействия органам Федеральной службы безопасности.

Запрещается использовать конфиденциальное содействие на контрактной основе депутатов, судей, прокуроров, адвокатов, несовершеннолетних, священнослужителей и полномочных представителей официально зарегистрированных религиозных организаций.

Сведения о лицах, оказывающих или оказывавших органам Федеральной службы безопасности содействие на конфиденциальной основе, составляют государственную тайну и могут быть преданы гласности только с письменного согласия этих лиц и в случаях, предусмотренных федеральными законами.

**Статья 20. Информационное обеспечение органов Федеральной службы безопасности**

Для осуществления своей деятельности органы Федеральной службы безопасности могут без лицензирования разрабатывать, создавать и эксплуатировать информационные системы, системы связи и системы передачи данных, а также средства защиты информации, включая средства криптографической защиты.

Наличие в информационных системах сведений о физических и юридических лицах не является основанием для принятия органами Федеральной службы безопасности мер, ограничивающих права указанных лиц.

Порядок учета и использования информации о совершенных правонарушениях, затрагивающих вопросы обеспечения безопасности Российской Федерации, а также сведений о разведывательной и иной деятельности специальных служб и организаций иностранных государств, отдельных лиц, направленной на нанесение ущерба безопасности Российской Федерации, устанавливается нормативными актами Федеральной службы безопасности Российской Федерации.

**Статья 21. Средства вооружения и оснащения органов Федеральной службы безопасности**

Органы Федеральной службы безопасности без лицензирования разрабатывают, создают, приобретают и используют средства вооружения и оснащения, включая специальные технические и иные средства, приобретают и используют боевое оружие, принятое на вооружение органов Федеральной службы безопасности решением Правительства Российской Федерации, а также другое служебное и гражданское оружие и боеприпасы к нему.

Продажа, передача, вывоз за пределы Российской Федерации и ввоз на ее территорию средств вооружения и оснащения, включая специальные технические и иные средства, огнестрельного оружия и боеприпасов к нему, которые могут использоваться в деятельности органов Федеральной службы безопасности, осуществляются ими в порядке, устанавливаемом Правительством Российской Федерации.

**Статья 22. Финансовое и материально-техническое обеспечение**

Финансирование органов Федеральной службы безопасности осуществляется за счет средств федерального бюджета.

Материально-техническое обеспечение органов Федеральной службы безопасности осуществляется за счет централизованных ресурсов Российской Федерации, а также за счет приобретения необходимых материально-технических средств у предприятий, учреждений и организаций независимо от форм собственности.

Земельные участки и имущество органов Федеральной службы безопасности (в том числе здания, сооружения, оборудование), созданное (создаваемое) или приобретенное (приобретаемое) за счет средств федерального бюджета и иных средств, являются федеральной собственностью. Органы Федеральной службы безопасности освобождаются от всех форм платы за землю с занимаемых ими земельных участков.

Органы Федеральной службы безопасности могут иметь служебный жилищный фонд, формируемый в порядке, устанавливаемом Правительством Российской Федерации.

Предприятия, учреждения и организации, созданные или создаваемые для обеспечения деятельности органов Федеральной службы безопасности, осуществляют свою деятельность без лицензирования и приватизации **не** подлежат.

**Глава V. Контроль и надзор за деятельностью органов Федеральной службы безопасности**

**Статья 23. Контроль за деятельностью органов Федеральной службы безопасности**

Контроль за деятельностью органов Федеральной службы безопасности осуществляют Президент Российской Федерации, Федеральное Собрание Российской Федерации, Правительство Российской Федерации и судебные органы в пределах полномочий, определяемых Конституцией Российской Федерации, федеральными конституционными законами и федеральными законами.

Депутаты (члены) Совета Федерации и депутаты Государственной Думы Федерального Собрания Российской Федерации в связи с осуществлением ими депутатской деятельности вправе получать сведения о деятельности органов Федеральной службы безопасности в порядке, определяемом законодательством Российской Федерации.

**Статья 24. Прокурорский надзор**

Надзор за исполнением органами Федеральной службы безопасности законов Российской Федерации осуществляют Генеральный прокурор Российской Федерации и уполномоченные им прокуроры.

Сведения о лицах, оказывающих или оказывавших органам Федеральной службы безопасности содействие на конфиденциальной основе, а также об организации, о тактике, методах и средствах осуществления деятельности

органов Федеральной службы безопасности в предмет прокурорского надзора не входят.

**Глава VI. Заключительные положения**

**Статья 25. О правопреемниках органов Федеральной службы безопасности**

Федеральная служба безопасности Российской Федерации и подчиненные ей органы являются правопреемниками Федеральной службы контрразведки Российской Федерации и ее органов.

Военнослужащие и гражданский персонал органов контрразведки Российской Федерации считаются проходящими военную службу (работающими) в органах Федеральной службы безопасности в занимаемых должностях без их переаттестации и переназначения, а также без проведения организационно-штатных мероприятий.

**Статья 26. Вступление настоящего Федерального закона в силу**

Настоящий Федеральный закон вступает в силу со дня его официального опубликования.

Признать утратившим силу со дня введения в действие настоящего Федерального закона Закон Российской Федерации «О федеральных органах государственной безопасности» (Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации, 1992, № 32, ст. 1871; 1993, № 33, ст. 1308; № 36, ст. 1438).

Предложить Президенту Российской Федерации и поручить Правительству Российской Федерации привести их нормативные правовые акты в соответствие с настоящим Федеральным законом.

**Москва, Кремль**

**3 апреля 1995 г.**

**Президент Российской Федерации Ельцин Б.**

**«О СЕРТИФИКАЦИИ ПРОДУКТОВ И УСЛУГ» Закон РФ от 10 июня 1993 г. № 5151-1 (в ред. Федерального закона от 27 декабря 1995 г. № 211-ФЗ)**

Настоящий Закон устанавливает правовые основы обязательной и добровольной сертификации продукции, услуг и иных объектов (далее — продукция) в Российской Федерации, а также права, обязанности и ответственность участников сертификации.

**Раздел I. Общие положения**

**Статья 1. Понятие сертификации**

Сертификация продукции (далее — сертификация) — это деятельность по подтверждению соответствия продукции установленным требованиям. Сертификация осуществляется в целях:

>• создания условий для деятельности предприятий, учреждений, организаций и предпринимателей на едином товарном рынке Российской Федерации, а также для участия в международном экономическом, научно-техническом сотрудничестве и международной торговле;

>• содействия потребителям в компетентном выборе продукции;

>• защиты потребителя от недобросовестности изготовителя (продавца, исполнителя); контроля безопасности продукции для окружающей среды, жизни, здоровья и имущества;

>• подтверждения показателей качества продукции, заявленных изготовителем. Сертификация может иметь обязательный и добровольный характер.

**Статья 2. Законодательство Российской Федерации о сертификации**

Отношения в области сертификации регулируются настоящим Законом и издаваемыми с ним актами законодательства Российской Федерации.

**Статья 3. Международные договоры**

Если международным договором Российской Федерации установлены иные правила, чем те, которые содержатся в законодательстве Российской Федерации о сертификации, то применяются правила международного договора.

**Статья 4. Полномочия Комитета Российской Федерации по стандартизации,**

**метрологии и сертификации**

Комитет Российской Федерации по стандартизации, метрологии и сертификации (далее — Госстандарт России) в соответствии с настоящим Законом:

>• формирует и реализует государственную политику в области сертификации, устанавливает общие правила и рекомендации по проведению сертификации на территории Российской Федерации и опубликовывает официальную информацию о них;

**>•** проводит государственную регистрацию систем сертификации и знаков соответствия, действующих в Российской Федерации;

>• опубликовывает официальную информацию о действующих в Российской Федерации системах сертификации и знаках соответствия и представляет ее в установленном порядке в международные (региональные) организации по сертификации;

**>•** готовит в установленном порядке предложения о присоединении к международным (региональным) системам сертификации, а также может в установленном порядке заключать соглашения с международными (региональными) организациями о взаимном признании результатов сертификации;

**>•** представляет в установленном порядке Российскую Федерацию в международных (региональных) организациях по вопросам сертификации как национальный орган Российской Федерации по сертификации.

**Статья 5. Система сертификации**

1. Система сертификации создается государственными органами управления, предприятиями, учреждениями и организациями и представляет собой совокупность участников сертификации, осуществляющих сертификацию по правилам, установленным в этой системе в соответствии с настоящим Законом.

В систему сертификации могут входить предприятия, учреждения и организации независимо от форм собственности, а также общественные объединения.

В систему сертификации могут входить несколько систем сертификации однородной продукции.

2. Системы сертификации подлежат государственной регистрации в установленном Госстандартом России порядке.

**Статья 6. Сертификат и знак соответствия**

1. Сертификат соответствия (далее — сертификат) — документ, выданный по правилам системы сертификации для подтверждения соответствия сертифицированной продукции установленным требованиям.

Обязательной составной частью сертификата соответствия является сертификат пожарной безопасности.

Порядок организации и проведения сертификации продукции и услуг в области пожарной безопасности определяется Государственной противопожарной службой Министерства внутренних дел Российской Федерации по согласованию с федеральным органом исполнительной власти в области стандартизации, метрологии и сертификации (абзацы 2 и 3 введены Федеральным законом от 27.12.95 г. № 211-ФЗ).

2. Знак соответствия — зарегистрированный в установленном порядке знак, которым по правилам, установленным в данной системе сертификации, подтверждается соответствие маркированной им продукции установленным требованиям.

Порядок государственной регистрации знаков соответствия устанавливается Госстандартом России.

3. Правила применения знаков соответствия устанавливаются конкретной системой сертификации в соответствии с правилами, устанавливаемыми Госстандартом России.

**Раздел II. Обязательная сертификация**

**Статья 7. Обязательная сертификация**

1. Обязательная сертификация осуществляется в случаях, предусмотренных законодательными актами Российской Федерации.

2. Организация и проведение работ по обязательной сертификации возлагаются на Госстандарт России, а в случаях, предусмотренных законодательными актами Российской Федерации в отношении отдельных видов продукции, могут быть возложены на другие государственные органы управления Российской Федерации.

3. Формы обязательной сертификации продукции устанавливаются Госстандартом России либо другими государственными органами управления Российской Федерации, уполномоченными на то в соответствии с настоящей статьей, с учетом сложившейся международной и зарубежной практики.

4. Запрещается рекламировать продукцию, подлежащую обязательной сертификации, но не имеющую сертификата соответствия.

**Статья 8. Участники обязательной сертификации**

Участниками обязательной сертификации являются Госстандарт России, иные государственные органы управления Российской Федерации, уполномоченные проводить работы по обязательной сертификации, органы по сертификации, испытательные лаборатории (центры), изготовители (продавцы, исполнители) продукции, а также центральные органы систем сертификации, определяемые в необходимых случаях для организации и координации работ в системах сертификации однородной продукции.

Допускается участие в проведении работ по обязательной сертификации зарегистрированных некоммерческих (бесприбыльных) объединений (союзов), и организаций любых форм собственности при условии их аккредитации соответствующим государственным органом управления.

**Статья 9. Правомочия государственных органов управления**

Госстандарт России и другие государственные органы управления Российской Федерации, на которые законодательными актами Российской Федерации возлагаются организация и проведение работ по обязательной сертификации, в пределах своей компетенции:

>• создают системы сертификации однородной продукции и устанавливают правила процедуры и управления для проведения сертификации в этих системах;

>• осуществляют выбор способа подтверждения соответствия продукции требованиям нормативных документов (формы сертификации);

>• определяют центральные органы систем сертификации;

>• аккредитуют органы по сертификации и испытательные лаборатории (центры) и выдают им разрешения на право проведения определенных видов работ (лицензии на проведение определенных видов работ);

>• ведут государственный реестр участников и объектов сертификации; устанавливают правила признания зарубежных сертификатов, знаков соответствия и результатов испытаний; устанавливают правила аккредитации и выдачи лицензий на проведение работ по обязательной сертификации;

>• осуществляют государственный контроль и надзор и устанавливают порядок инспекционного контроля за соблюдением правил сертификации за сертифицированной продукцией;

>• рассматривают апелляции по вопросам сертификации;

>• выдают сертификаты и лицензии на применение знака соответствия.

**Статья 10. Обязанности центрального органа системы сертификации**

Центральный орган системы сертификации:

**>•** организует, координирует работу и устанавливает правила процедуры и управления в возглавляемой им системе сертификации;

>• рассматривает апелляции заявителей по поводу действий органов по сертификации, испытательных лабораторий (центров).

**Статья 11. Обязанности органа по сертификации**

Орган по сертификации:
>• сертифицирует продукцию, выдает сертификаты и лицензии на применение знака соответствия;
>• приостанавливает либо отменяет действие выданных им сертификатов;
>• предоставляет заявителю по его требованию необходимую информацию в пределах своей компетенции.

**Статья 12. Обязанности испытательной лаборатории (центра)**

Испытательные лаборатории (центры), аккредитованные в установленном соответствующей системой сертификации порядке, осуществляют испытания конкретной продукции или конкретные виды испытаний и выдают протоколы испытаний для целей сертификации.

**Статья 13. Обязанности изготовителей (продавцов, исполнителей)**

Изготовители (продавцы, исполнители) продукции, подлежащей обязательной сертификации и реализуемой на территории Российской Федерации, обязаны:
>• реализовывать эту продукцию только при наличии сертификата, выданного или признанного уполномоченным на то органом;
>• обеспечивать соответствие реализуемой продукции требованиям нормативных документов, на соответствие которым она была сертифицирована, и маркирование ее знаком соответствия в установленном порядке;
>• указывать в сопроводительной технической документации сведения о сертификации и нормативных документах, которым должна соответствовать продукция, и обеспечивать доведение этой информации до потребителя (покупателя, заказчика);
>• приостанавливать или прекращать реализацию сертифицированной продукции, если она не отвечает требованиям нормативных документов, на соответствие которым сертифицирована, по истечении срока действия сертификата или в случае, если действие сертификата приостановлено либо отменено решением органа по сертификации; обеспечивать беспрепятственное выполнение своих полномочий должностными лицами органов, осуществляющих обязательную сертификацию продукции и контроль за сертифицированной продукцией; извещать орган по сертификации в установленном им порядке об изменениях, внесенных в техническую документацию или в технологический процесс производства сертифицированной продукции.

**Статья 14. Условия ввоза импортируемой продукции**

1. В условиях контрактов (договоров), заключаемых на поставку в Российскую Федерацию продукции, подлежащей в соответствии с актами законодательства Российской Федерации обязательной сертификации, должно быть предусмотрено наличие сертификата и знака соответствия, подтверждающих ее соответствие установленным требованиям. Указанные сертификаты и знаки соответствия должны быть выданы или признаны уполномоченным на то органом Российской Федерации.
2. Сертификаты или свидетельства об их признании представляются в таможенные органы вместе с грузовой таможенной декларацией и являются необходимыми документами для получения разрешения на ввоз продукции на территорию Российской Федерации.
3. Порядок ввоза на территорию Российской Федерации продукции, подлежащей обязательной сертификации, устанавливается Государственным таможенным комитетом Российской Федерации и Госстандартом России в соответствии с законодательными актами Российской Федерации.

**Статья 15. Государственный контроль и надзор за соблюдением правил обязательной сертификации и за сертифицированной продукцией**

1. Государственный контроль и надзор за соблюдением изготовителями (продавцами, исполнителями), испытательными лабораториями (центрами), органами по сертификации правил обязательной сертификации и **за** сертифицированной продукцией осуществляется Госстандартом России, иными

специально уполномоченными государственными органами управления Российской Федерации в пределах их компетенции.
2. Непосредственно государственный контроль и надзор за соблюдением правил сертификации и сертифицированной продукцией проводится должностными лицами, осуществляющими государственный контроль и надзор за соблюдением обязательных требований государственных стандартов. Указанные должностные лица осуществляют государственный контроль и надзор за соблюдением правил по сертификации и за сертифицированной продукцией в порядке и на условиях, установленных Законом Российской Федерации «О стандартизации».

**Статья 16. Финансирование работ по сертификации и государственному контролю и надзору**

1. Обязательному государственному финансированию подлежат:
>• разработка прогнозов развития сертификации, правил и рекомендаций по ее проведению;
**>•** обеспечение официальной информацией в области сертификации;
>• участие в работе международных (региональных) организаций по сертификации и проведение работ с зарубежными национальными органами по сертификации;
>• разработка и (или) участие в разработке международных (региональных) правил и рекомендаций по сертификации;
>• разработка проектов актов законодательства в области сертификации;
>• проведение научно-исследовательских и иных работ по сертификации, имеющих общегосударственное значение;
>• проведение государственного контроля и надзора за соблюдением правил сертификации и за сертифицированной продукцией;
>• ведение Государственного реестра по сертификации и аккредитации и архивное хранение материалов по государственной регистрации систем сертификации и знаков соответствия;
>• другие работы по обязательной сертификации, определяемые законодательством Российской Федерации.
2. Оплата работ по обязательной сертификации конкретной продукции производится заявителем в порядке, установленном Госстандартом России и государственными органами управления Российской Федерации, на которые законодательными актами Российской Федерации возложены организация и проведение обязательной сертификации, по согласованию с Министерством финансов Российской Федерации. Сумма средств, израсходованных заявителем на проведение обязательной сертификации своей продукции, относится на ее себестоимость.

**Раздел III. Добровольная сертификация**

**Статья 17. Добровольная сертификация**

По продукции, не подлежащей в соответствии с законодательными актами Российской Федерации обязательной сертификации, и по требованиям, на соответствие которым законодательными актами Российской Федерации не предусмотрено проведение обязательной сертификации, по инициативе юридических лиц и граждан может проводиться добровольная сертификация на условиях договора между заявителем и органом по сертификации.

**Статья 18. Организация добровольной сертификации**

Добровольную сертификацию вправе осуществлять любое юридическое лицо, взявшее на себя функцию органа по добровольной сертификации и зарегистрировавшее систему сертификации и знак соответствия в Госстандарте России в установленном Госстандартом России порядке. Органы по обязательной сертификации также вправе проводить добровольную сертификацию при соблюдении указанных условий.
Орган по добровольной сертификации устанавливает правила проведения работ в системе сертификации, в том числе порядок их оплаты.

**Статья 19. Права заявителя**

При заключении договора на проведение сертификации заявитель вправе получить от органа по добровольной сертификации необходимую информацию о правилах сертификации продукции, а также определить форму сертификации.

**Раздел IV. Ответственность за нарушение положении настоящего Закона**

**Статья 20. Уголовная, административная либо гражданско-правовая ответственность**

Юридические и физические лица, а также органы государственного управления, виновные в нарушении правил обязательной сертификации, несут в соответствии с действующим законодательством уголовную, административную либо гражданско-правовую ответственность.

**Президент Российской Федерации Б. Ельцин**

«О СТАНДАРТИЗАЦИИ» Закон РФ от 10 июня 1993 г. № 5154-1 (в ред. Федерального закона от 27 декабря 1995 г. № 211-ФЗ)

Настоящий Закон устанавливает правовые основы стандартизации в Российской Федерации, обязательные для всех государственных органов управления, а также предприятий и предпринимателей (далее — субъекты хозяйственной деятельности), общественных объединений, и определяет меры государственной защиты интересов потребителей и государства посредством разработки и применения нормативных документов по стандартизации.

**Раздел I. Общие положения**

**Статья 1. Понятие стандартизации**

Стандартизация — это деятельность по установлению норм, правил и характеристик (далее -- требования) в целях обеспечения:

>• безопасности продукции, работ и услуг для окружающей среды, жизни, здоровья и имущества; технической и информационной совместимости, а также взаимозаменяемости продукции;

**>•** качества продукции, работ и услуг в соответствии с уровнем развития науки, техники и технологии; единства измерений;

>• экономии всех видов ресурсов;

>• безопасности хозяйственных объектов с учетом риска возникновения природных и техногенных катастроф и других чрезвычайных ситуаций;

**>•** обороноспособности и мобилизационной готовности страны.

**Статья 2. Законодательство Российской Федерации о стандартизации**

Отношения в области стандартизации регулируются настоящим Законом и издаваемыми в соответствии с ним актами законодательства Российской Федерации.

Настоящий Закон не регулирует отношения, связанные с государственными образовательными стандартами.

**Статья 3. Международные договоры**

Если международным договором Российской Федерации установлены иные правила, чем те, которые содержатся в законодательстве Российской Федерации о стандартизации, то применяются правила международного договора.

**Статья 4. Организация работ по стандартизации**

1. Государственное управление стандартизацией в Российской Федерации, включая координацию деятельности государственных органов управления Российской Федерации, взаимодействие с органами власти республик в составе Российской Федерации, краев, областей, автономной области, автономных округов, городов, с общественными объединениями, в том числе с техническими комитетами по стандартизации, с субъектами хозяйственной деятельности, осуществляет Комитет Российской Федерации по стандартизации, метрологии и сертификации (Госстандарт России).

Госстандарт России формирует и реализует государственную политику в области стандартизации, осуществляет государственный контроль и надзор за соблюдением обязательных требований государственных стандартов,

участвует в работах по международной (региональной) стандартизации, организует профессиональную подготовку и переподготовку кадров в области стандартизации, а также устанавливает правила применения международных (региональных) стандартов, правил, норм и рекомендаций по стандартизации на территории Российской Федерации, если иное не установлено международными договорами Российской Федерации.

Другие государственные органы управления участвуют в работах по стандартизации в пределах их компетенции.

Субъекты хозяйственной деятельности, включая общественные объединения, организуют и проводят работы по стандартизации в соответствии с настоящим Законом.

2. Госстандарт России в соответствии с настоящим Законом устанавливает в государственных стандартах государственной системы стандартизации общие организационно-технические правила проведения работ по стандартизации, формы и методы взаимодействия субъектов хозяйственной деятельности друг с другом, с государственными органами управления.

**Статья 5. Международное сотрудничество в области стандартизации**

Госстандарт России вправе представлять Российскую Федерацию в международных (региональных) организациях, осуществляющих деятельность **по** стандартизации.

**Раздел II. Нормативные документы по стандартизации и их применение**

**Статья 6. Нормативные документы по стандартизации и требования к ним**

1. К нормативным документам по стандартизации, действующим на территории Российской Федерации в случаях, порядке и на условиях, установленных настоящим Законом, относятся:

>• государственные стандарты Российской Федерации (далее — государственные стандарты);

>• применяемые в установленном порядке международные (региональные) стандарты, правила, нормы и рекомендации по стандартизации;

>• общероссийские классификаторы технико-экономической информации; стандарты отраслей; стандарты предприятий;

>• стандарты научно-технических, инженерных обществ и других общественных объединений.

Под отраслью в настоящем Законе понимается совокупность субъектов хозяйственной деятельности независимо от их ведомственной принадлежности и форм собственности, разрабатывающих и (или) производящих продукцию (выполняющих работы и оказывающих услуги) определенных видов, которые имеют однородное потребительное или функциональное назначение.

2. Требования, устанавливаемые нормативными документами по стандартизации, должны основываться на современных достижениях науки, техники и технологии, международных (региональных) стандартах, правилах, нормах и рекомендациях по стандартизации, прогрессивных национальных стандартах других государств, учитывать условия использования продукции, выполнения работ и оказания услуг, условия и режимы труда и не должны нарушать положений, установленных актами законодательства Российской Федерации.

3. Нормативные документы по стандартизации на продукцию и услуги, подлежащие в соответствии с законодательством обязательной сертификации, должны содержать требования, по которым осуществляется обязательная сертификация, методы контроля на соответствие этим требованиям, правила маркировки продукции и услуг, требования к информации о сертификации, включаемой в сопроводительную документацию.

Нормативные документы по стандартизации, которые принимаются федеральными органами исполнительной власти и устанавливают или должны устанавливать требования пожарной безопасности, подлежат обязательному согласованию с Государственной противопожарной службой Министерства

внутренних дел Российской Федерации (абзац введен Федеральным законом от 27.12.95 г. № 211-ФЗ).

4. Государственные стандарты, стандарты отраслей не являются объектом авторского права.

**Статья 7. Государственные стандарты, общероссийские классификаторы технико-экономической информации**

1. Государственные стандарты разрабатываются на продукцию, работы и услуги, имеющие межотраслевое значение, и не должны противоречить законодательству Российской Федерации. Государственные стандарты должны содержать:

>• требования к продукции, работам и услугам по их безопасности для окружающей среды, жизни, здоровья и имущества, требования пожарной безопасности, требования техники безопасности и производственной санитарии (в ред. Федерального закона от 27.12.95 г. № 211-ФЗ);

>• требования по технической и информационной совместимости, а также взаимозаменяемости продукции;

>• основные потребительские (эксплуатационные) характеристики продукции, методы их контроля, требования к упаковке, маркировке, транспортированию, хранению, применению и утилизации продукции;

>• правила и нормы, обеспечивающие техническое и информационное единство при разработке, производстве, использовании (эксплуатации) продукции, выполнении работ и оказании услуг, в том числе правила оформления технической документации, допуски и посадки, общие правила обеспечения качества продукции, работ и услуг, сохранения и рационального использования всех видов ресурсов, термины и их определения, условные обозначения, метрологические и другие общетехнические и организационно — технические правила и нормы.

Для обеспечения государственной защиты интересов Российской Федерации и конкурентоспособности отечественной продукции (услуг) в государственных стандартах в обоснованных случаях устанавливаются предварительные требования на перспективу, опережающие возможности традиционных технологий.

Содержание требований государственных стандартов, области их распространения, сферы их действия и даты их введения определяются государственными органами управления, которые их принимают.

2. Требования, устанавливаемые государственными стандартами для обеспечения безопасности продукции, работ и услуг для окружающей среды, жизни, здоровья и имущества, для обеспечения технической и информационной совместимости, взаимозаменяемости продукции, единства методов их контроля и единства маркировки, а также иные требования, установленные законодательством Российской Федерации, являются обязательными для соблюдения государственными органами управления, субъектами хозяйственной деятельности.

Соответствие продукции и услуг указанным требованиям государственных стандартов определяется в порядке, установленном законодательством Российской Федерации об обязательной сертификации продукции и услуг.

Иные требования государственных стандартов к продукции, работам и услугам подлежат обязательному соблюдению субъектами хозяйственной деятельности в силу договора либо в том случае, если об этом указывается в технической документации изготовителя (поставщика) продукции, исполнителя работ или услуг. При этом соответствие продукции и услуг этим требованиям государственных стандартов может определяться в порядке, установленном законодательством Российской Федерации о добровольной сертификации продукции и услуг.

3. Соответствие продукции и услуг требованиям государственных стандартов может подтверждаться путем маркирования продукции и услуг знаком соответствия государственным стандартам.

Форму знака соответствия государственным стандартам, порядок маркирования этим знаком, а также порядок выдачи субъектам хозяйственной деятельности лицензий на маркирование ими продукции и услуг этим знаком устанавливает Госстандарт России.
Субъекты хозяйственной деятельности, которым выданы лицензии на маркирование продукции и услуг знаком соответствия государственным стандартам, а также сами продукция и услуги, маркированные этим знаком, вносятся в Государственный реестр продукции и услуг, маркированных знаком соответствия государственным стандартам. Порядок ведения указанного реестра и пользования им устанавливает Госстандарт России.
4. В соответствии с настоящим Законом государственные стандарты и общероссийские классификаторы технико-экономической информации принимает Госстандарт России, а в области строительства и промышленности строительных материалов — Государственный комитет Российской Федерации по вопросам архитектуры и строительства (Госстрой России).
Государственные стандарты вводятся в действие после их государственной регистрации в Госстандарте России.
5. Порядок разработки, принятия, введения в действие, применения и ведения общероссийских классификаторов технико-экономической информации устанавливает Госстандарт России.

**Статья 8. Стандарты отраслей, стандарты предприятий, стандарты научно-технических, инженерных обществ и других общественных объединений**

1. Стандарты отраслей могут разрабатываться и приниматься государственными органами управления в пределах их компетенции в целях обеспечения требований, указанных в статье 1 настоящего Закона применительно к продукции, работам и услугам отраслевого значения.
Стандарты отраслей не должны нарушать обязательные требования государственных стандартов.
Ответственность за соответствие требований стандартов отраслей обязательным требованиям государственных стандартов несут принявшие их государственные органы управления.
Порядок разработки, принятия, учетной регистрации, применения, контроля за соблюдением обязательных требований, изменения и отмены стандартов отраслей устанавливается государственными стандартами Государственной системы стандартизации.
2. Стандарты предприятий могут разрабатываться и утверждаться предприятиями самостоятельно, исходя из необходимости их применения в целях обеспечения требований, указанных в статье 1 настоящего Закона, а также в целях совершенствования организации и управления производством.
Требования стандартов предприятий подлежат обязательному соблюдению другими субъектами хозяйственной деятельности, если в договоре на разработку, производство и поставку продукции, на выполнение работ и оказание услуг сделана ссылка на эти стандарты.
3. Стандарты научно-технических, инженерных обществ и других общественных объединений разрабатываются и принимаются этими общественными объединениями для динамичного распространения и использования полученных в различных областях знаний результатов исследований и разработок. Необходимость применения этих стандартов субъекты хозяйственной деятельности определяют самостоятельно.
4. Порядок разработки, утверждения, учета, изменения и отмены стандартов субъектов хозяйственной деятельности устанавливается ими самостоятельно в соответствии с настоящим Законом.
5. Стандарты субъектов хозяйственной деятельности не должны нарушать обязательные требования государственных стандартов.
Ответственность за соответствие требований стандартов субъектов хозяйственной деятельности обязательным требованиям государственных

стандартов несут утвердившие их субъекты хозяйственной деятельности.
6. Информация о принятых стандартах отраслей, стандартах научно-технических, инженерных обществ и других общественных объединений направляется в органы Госстандарта России.

**Статья 9. Применение нормативных документов по стандартизации**

1. Нормативные документы по стандартизации должны применяться государственными органами управления, субъектами хозяйственной деятельности на стадиях разработки, подготовки продукции к производству, ее изготовления, реализации (поставки, продажи), использования (эксплуатации), хранения, транспортирования и утилизации, при выполнении работ и оказании услуг, при разработке технической документации (конструкторской, технологической, проектной), в том числе технических условий, каталожных листов на поставляемую продукцию (оказываемые услуги).

При этом действующие отраслевые стандарты применяются на территории Российской Федерации в случаях, если их требования не противоречат законодательству Российской Федерации.

2. Заказчик и исполнитель обязаны включать в договор условие о соответствии продукции, выполняемых работ и оказываемых услуг обязательным требованиям государственных стандартов.

3. Необходимость применения нормативных документов по стандартизации в отношении продукции (услуг), производимой (оказываемых) на территории Российской Федерации с целью вывоза с ее территории определяется контрактом (договором), за исключением случаев, установленных законодательством Российской Федерации.

4. Ввоз продукции и услуг на таможенную территорию Российской Федерации, а также подтверждение их соответствия обязательным требованиям государственных стандартов осуществляются в порядке, установленном законодательством Российской Федерации.

**Статья 10. Информация о нормативных документах по стандартизации, их издание и реализация**

1. Официальная информация о разрабатываемых и принятых государственных стандартах, общероссийских классификаторах технико-экономической информации, а также сами эти государственные стандарты и общероссийские классификаторы должны быть доступны для пользователей, в том числе зарубежных, в той части, в которой они не составляют государственной тайны.

2. Госстандарт России организует публикацию официальной информации о государственных стандартах, общероссийских классификаторах технико-экономической информации, международных (региональных) стандартах, правилах, нормах и рекомендациях по стандартизации, национальных стандартах других государств, а также информации о международных договорах в области стандартизации и правилах их применения; создает и ведет федеральный фонд государственных стандартов и общероссийских классификаторов технико-экономической информации, а также международных (региональных) стандартов, правил, норм и рекомендаций по стандартизации, национальных стандартов зарубежных стран. Порядок создания и правила пользования этим фондом устанавливаются Правительством Российской Федерации.

3. Государственные органы управления, принявшие в пределах своей компетенции нормативные документы по стандартизации, субъекты хозяйственной деятельности, утвердившие нормативные документы по стандартизации, формируют и ведут информационные фонды этих документов, а также обеспечивают пользователей информацией о них и самими документами на договорной основе.

4. Исключительное право официального опубликования в установленном порядке государственных стандартов и общероссийских классификаторов

технико-экономической информации принадлежит государственным органам управления, принявшим эти нормативные документы по стандартизации.
Порядок опубликования государственных стандартов и общероссийских классификаторов технико-экономической информации определяется Правительством Российской Федерации.
5. Исключительное право официального опубликования сведений, содержащихся в Общероссийском каталоге продукции и услуг, внесенных в Государственный реестр продукции и услуг, маркированных знаком соответствия государственным стандартам, принадлежит Госстандарту России.

**Раздел III. Государственный контроль и надзор за соблюдением требований государственных стандартов**

**Статья 11. Государственный контроль и надзор**

1. Государственный контроль и надзор за соблюдением субъектами хозяйственной деятельности обязательных требований государственных стандартов осуществляется на стадиях разработки, подготовки продукции к производству, ее изготовления, реализации (поставки, продажи), использования (эксплуатации), хранения, транспортирования и утилизации, а также при выполнении работ и оказании услуг.
2. Порядок осуществления государственного контроля и надзора за соблюдением обязательных требований государственных стандартов устанавливает Госстандарт России в соответствии с законодательством Российской Федерации.
3. Должностные лица субъектов хозяйственной деятельности обязаны создавать все условия, необходимые для осуществления государственного контроля и надзора.

**Статья 12. Органы государственного контроля и надзора**

1. Органами, осуществляющими государственный контроль и надзор за соблюдением обязательных требований государственных стандартов, являются Госстандарт России, иные специально уполномоченные государственные органы управления в пределах их компетенции.
2. Осуществление государственного контроля и надзора за соблюдением обязательных требований государственных стандартов проводится должностными лицами государственных органов управления в пределах их компетенции.
Непосредственное осуществление государственного контроля и надзора за соблюдением обязательных требований государственных стандартов от имени Госстандарта России проводится его должностными лицами — государственными инспекторами:
**>•** главным государственным инспектором Российской Федерации по надзору за государственными стандартами;
**>•** главными государственными инспекторами республик в составе Российской Федерации, краев, областей, автономной области, автономных округов, городов по надзору за государственными стандартами;
>• государственными инспекторами по надзору за государственными стандартами.

**Статья 13. Государственные инспекторы, их права и ответственность**

1. Государственные инспекторы, осуществляющие государственный контроль и надзор за соблюдением обязательных требований государственных стандартов, являются представителями государственных органов управления и находятся под защитой государства. Государственный инспектор имеет право:
>• свободного доступа в служебные и производственные помещения субъекта хозяйственной деятельности; получать от субъекта хозяйственной деятельности документы и сведения, необходимые для проведения государственного контроля и надзора;
>• использовать технические средства и специалистов субъекта

хозяйственной деятельности при проведении государственного контроля и надзора;

>• проводить в соответствии с действующими нормативными документами по стандартизации отбор проб и образцов продукции и услуг для контроля их соответствия обязательным требованиям государственных стандартов с отнесением стоимости израсходованных.

**«ОБ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ» Федеральный закон от 12 августа 1995 г. ЛЬ 144-ФЗ (с изменениями от 18 июля 1997 г.) Принят Государственной Думой 5 июля 1995 г.**

Настоящий Федеральный закон определяет содержание оперативно-розыскной деятельности, осуществляемой на территории Российской Федерации, и закрепляет систему гарантий законности при проведении оперативно-розыскных мероприятий.

**Глава I. Общие положения**

**Статья 1. Оперативно-розыскная деятельность**

Оперативно-розыскная деятельность — вид деятельности, осуществляемой гласно и негласно оперативными подразделениями государственных органов, уполномоченных на то настоящим Федеральным законом (далее — органы, осуществляющие оперативно-розыскную деятельность), в пределах их полномочий посредством проведения оперативно-розыскных мероприятий в целях защиты жизни, здоровья, прав и свобод человека и гражданина, собственности, обеспечения безопасности общества и государства от преступных посягательств.

**Статья 2. Задачи оперативно-розыскной деятельности**

Задачами оперативно-розыскной деятельности являются:

>• выявление, предупреждение, пресечение и раскрытие преступлений, а также выявление и установление лиц, их подготавливающих, совершающих или совершивших;

>• осуществление розыска лиц, скрывающихся от органов дознания, следствия и суда, уклоняющихся от уголовного наказания, а также розыска без вести пропавших;

>• добывание информации о событиях или действиях, создающих угрозу государственной, военной, экономической или экологической безопасности Российской Федерации.

**Статья 3. Принципы оперативно-розыскной деятельности**

Оперативно-розыскная деятельность основывается на конституционных принципах законности, уважения и соблюдения прав и свобод человека и гражданина, а также на принципах конспирации, сочетания гласных и негласных методов и средств.

**Статья 4. Правовая основа оперативно-розыскной деятельности**

Правовую основу оперативно-розыскной деятельности составляют Конституция Российской Федерации, настоящий Федеральный закон, другие федеральные законы и принятые в соответствии с ними иные нормативные правовые акты федеральных органов государственной власти.

Органы, осуществляющие оперативно-розыскную деятельность, издают в пределах своих полномочий в соответствии с законодательством Российской Федерации нормативные акты, регламентирующие организацию и тактику проведения оперативно-розыскных мероприятий.

**Статья 5. Соблюдение прав и свобод человека и гражданина при осуществлении оперативно-розыскной деятельности**

Не допускается осуществление оперативно-розыскной деятельности для достижения целей и решения задач, не предусмотренных настоящим Федеральным законом.

Лицо, полагающее, что действия органов, осуществляющих оперативно-розыскную деятельность, привели к нарушению его прав и свобод, вправе обжаловать, эти действия в вышестоящий орган, осуществляющий оперативно-розыскную деятельность, прокурору или в суд.

Лицо, виновность которого в совершении преступления не доказана в установленном законом порядке, то есть в отношении которого в возбуждении уголовного дела отказано либо уголовное дело прекращено в связи с отсутствием события преступления или в связи с отсутствием в деянии состава преступления, и которое располагает фактами проведения в отношении его оперативно-розыскных мероприятий и полагает, что при этом были нарушены его права, вправе истребовать от органа, осуществляющего оперативно-розыскную деятельность, сведения о полученной о нем информации в пределах, допускаемых требованиями конспирации и исключающих возможность разглашения государственной тайны. В случае, если будет отказано в предоставлении запрошенных сведений или если указанное лицо полагает, что сведения получены не в полном объеме, оно вправе обжаловать это в судебном порядке. В процессе рассмотрения дела в суде обязанность доказывать обоснованность отказа в предоставлении этому лицу сведений, в том числе в полном объеме, возлагается на соответствующий орган, осуществляющий оперативно-розыскную деятельность.

В целях обеспечения полноты и всесторонности рассмотрения дела орган, осуществляющий оперативно-розыскную деятельность, обязан предоставить судье по его требованию оперативно-служебные документы» содержащие информацию о сведениях, в предоставлении которых было отказано заявителю, за исключением сведений о лицах, внедренных в организованные преступные группы, о штатных негласных сотрудниках органов, осуществляющих оперативно-розыскную деятельность, и о лицах, оказывающих им содействие на конфиденциальной основе.

В случае признания необоснованным решения органа, осуществляющего оперативно-розыскную деятельность, об отказе в предоставлении необходимых сведений заявителю судья может обязать указанный орган предоставить заявителю сведения, предусмотренные частью третьей настоящей статьи.

Полученные в результате проведения оперативно-розыскных мероприятий материалы в отношении лиц, виновность которых в совершении преступления не доказана в установленном законом порядке, хранятся один год, а затем уничтожаются, если служебные интересы или правосудие не требуют иного. За три месяца до дня уничтожения материалов, отражающих результаты оперативно-розыскных мероприятий, проведенных на основании судебного решения, об этом уведомляется соответствующий судья.

Органам (должностным лицам), осуществляющим оперативно-розыскную деятельность, запрещается:

>• проводить оперативно-розыскные мероприятия в интересах какой-либо политической партии, общественного и религиозного объединения;

>• принимать негласное участие в работе федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, а также в деятельности зарегистрированных в установленном порядке и незапрещенных политических партий, общественных и религиозных объединений в целях оказания влияния на характер их деятельности;

>• разглашать сведения, которые затрагивают неприкосновенность частной жизни, личную и семейную тайну, честь и доброе имя граждан и которые стали известными в процессе проведения оперативно-розыскных мероприятий, без согласия граждан, за исключением случаев, предусмотренных федеральными законами.

При нарушении органом (должностным лицом), осуществляющим оперативно-розыскную деятельность, прав и законных интересов физических и юридических лиц вышестоящий орган, прокурор либо судья в соответствии с законодательством Российской Федерации обязаны принять меры по восстановлению этих прав и законных интересов, возмещению причиненного

вреда.
Нарушения настоящего Федерального закона при осуществлении оперативно-розыскной деятельности влекут ответственность, предусмотренную законодательством Российской Федерации.

**Глава II. Проведение оперативно-розыскных мероприятии**

**Статья 6. Оперативно-розыскные мероприятия**

При осуществлении оперативно-розыскной деятельности проводятся следующие оперативно-розыскные мероприятия:

1. Опрос граждан.
2. Наведение справок.
3. Сбор образцов для сравнительного исследования.
4. Проверочная закупка.
5. Исследование предметов и документов.
6. Наблюдение.
7. Отождествление личности.
8. Обследование помещений, зданий, сооружений, участков местности и транспортных средств.
9. Контроль почтовых отправлений, телеграфных и иных сообщений.
10. Прослушивание телефонных переговоров.
11. Снятие информации с технических каналов связи.
12. Оперативное внедрение.
13. Контролируемая поставка.
14. Оперативный эксперимент.

Приведенный перечень оперативно-розыскных мероприятий может быть изменен или дополнен только Федеральным законом.

В ходе проведения оперативно-розыскных мероприятий используются информационные системы, видео- и аудиозапись, кино- и фотосъемка, а также другие технические и иные средства, не наносящие ущерб жизни и здоровью людей и не причиняющие вред окружающей среде.

Оперативно-розыскные мероприятия, связанные с контролем почтовых отправлений, телеграфных и иных сообщений, прослушиванием телефонных переговоров с подключением к станционной аппаратуре предприятий, у учреждений и организаций независимо от форм собственности, физических и юридических лиц, предоставляющих услуги и средства связи, со снятием информации с технических каналов связи, проводятся с использованием оперативно-технических сил и средств органов Федеральной службы безопасности и органов внутренних дел в порядке, определяемом межведомственными нормативными актами или соглашениями между органами, осуществляющими оперативно-розыскную деятельность.

См. Технические требования к системе технических средств по обеспечению функций оперативно-розыскных мероприятий на электронных АТС (СОРМ), утвержденные Минсвязи РФ 19 сентября 1994 г. (приложение к письму Минсвязи РФ от 11 ноября 1994 г. № 252-У).

О взаимодействии предприятий связи с органами, осуществляющими ОРД, см. Федеральный закон от 16 февраля 1995 г. NB 15-ФЗ «О связи».

Должностные лица органов, осуществляющих оперативно-розыскную деятельность, решают ее задачи посредством личного участия в организации и проведении оперативно-розыскных мероприятий, используя помощь должностных лиц и специалистов, обладающих научными, техническими и иными специальными знаниями, а также отдельных граждан с их согласия на гласной и негласной основе.

Запрещается проведение оперативно-розыскных мероприятий и использование специальных и иных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации, не уполномоченными на то настоящим Федеральным законом физическими и юридическими лицами.

Разработка, производство, реализация, приобретение в целях продажи,

ввоз в Российскую Федерацию и вывоз за ее пределы специальных технических средств, предназначенных для негласного получения информации, не уполномоченными на осуществление оперативно-розыскной деятельности физическими и юридическими лицами подлежат лицензированию в порядке, устанавливаемом Правительством Российской Федерации.
О порядке лицензирования указанной деятельности см. постановление Правительства РФ от 1 июля 1996 г. NQ 770.
Перечень видов специальных технических средств, предназначенных для негласного получения информации в процессе осуществления оперативно-розыскной деятельности устанавливается Правительством Российской Федерации.
Указанный перечень утвержден постановлением Правительства РФ от 1 июля 1996 г. № 7JO.

**Статья 7. Основания для проведения оперативно-розыскных мероприятий**

Основаниями для проведения оперативно-розыскных мероприятий являются:
1. Наличие возбужденного уголовного дела.
2. Ставшие известными органам, осуществляющим оперативно-розыскную деятельность, сведения о:
1) признаках подготавливаемого, совершаемого или совершенного противоправного деяния, а также о лицах, его подготавливающих, совершающих или совершивших, если нет достаточных данных для решения вопроса о возбуждении уголовного дела;
2) событиях или действиях, создающих угрозу государственной, военной, экономической или экологической безопасности Российской Федерации;
3) лицах, скрывающихся от органов дознания, следствия и суда или уклоняющихся от уголовного наказания;
4) лицах, без вести пропавших, и об обнаружении неопознанных трупов.
3. Поручения следователя, органа дознания, указания прокурора или определения суда по уголовным делам, находящимся в их производстве.
4. Запросы других органов, осуществляющих оперативно-розыскную деятельность, по основаниям, указанным в настоящей статье.
5. Постановление о применении мер безопасности в отношении защищаемых лиц, осуществляемых уполномоченными на то государственными органами в порядке, предусмотренном законодательством Российской Федерации.
6. Запросы международных правоохранительных организаций и правоохранительных органов иностранных государств в соответствии с международными договорами Российской Федерации.
Органы, осуществляющие оперативно-розыскную деятельность, в пределах своих полномочий вправе также собирать данные, необходимые для принятия решений:
1. О допуске к сведениям, составляющим государственную тайну.
2. О допуске к работам, связанным с эксплуатацией объектов, представляющих повышенную опасность для жизни и здоровья людей, а также для окружающей среды.
3. О допуске к участию в оперативно-розыскной деятельности или о доступе к материалам, полученным в результате ее осуществления.
4. Об установлении или о поддержании с лицом отношений сотрудничества при подготовке и проведении оперативно-розыскных мероприятий.
5. По обеспечению безопасности органов, осуществляющих оперативно-розыскную деятельность.
6. О выдаче разрешений на частную детективную и охранную деятельность.

**Статья 8. Условия проведения оперативно-розыскных мероприятий**

Гражданство, национальность, пол, место жительства, имущественное, должностное и социальное положение, принадлежность к общественным объединениям, отношение к религии и политические убеждения отдельных лиц не являются препятствием для проведения в отношении их оперативно-розыскных мероприятий на территории Российской Федерации, если иное не

предусмотрено федеральным законом.
Проведение оперативно-розыскных мероприятий, которые ограничивают конституционные права граждан на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, а также право на неприкосновенность жилища, допускается на основании судебного решения и при наличии информации:
1. О признаках подготавливаемого, совершаемого или совершенного противоправного деяния, по которому производство предварительного следствия обязательно.
2. О лицах, подготавливающих, совершающих или совершивших противоправное деяние, по которому производство предварительного следствия обязательно.
3. О событиях или действиях, создающих угрозу государственной, военной экономической или экологической безопасности Российской Федерации.
В случаях, которые не терпят отлагательства и могут привести к совершению тяжкого преступления, а также при наличии данных о событиях и действиях, создающих угрозу государственной, военной, экономической или экологической безопасности Российской Федерации, на основании мотивированного постановления одного из руководителей органа, осуществляющего оперативно-розыскную деятельность, допускается проведение оперативно-розыскных мероприятий, предусмотренных частью второй настоящей статьи, с обязательным уведомлением суда (судьи) в течение 24 часов. В течение 48 часов с момента начала проведения оперативно-розыскного мероприятия орган, его осуществляющий, обязан получить судебное решение о проведении такого оперативно-розыскного мероприятия либо прекратить его проведение.
В случае возникновения угрозы жизни, здоровью, собственности отдельных лиц по их заявлению или с их согласия в письменной форме разрешается прослушивание переговоров, ведущихся с их телефонов, на основании постановления, утвержденного руководителем органа, осуществляющего оперативно-розыскную деятельность, с обязательным уведомлением соответствующего суда (судьи) в течение 48 часов.
Проверочная закупка или контролируемая поставка предметов, веществ и продукции, свободная реализация которых запрещена либо оборот которых ограничен, а также оперативный эксперимент или оперативное внедрение должностных лиц органов, осуществляющих оперативно-розыскную деятельность, а равно лиц, оказывающих им содействие, проводятся на основании постановления, утвержденного руководителем органа, осуществляющего оперативно-розыскную деятельность.
Проведение оперативного эксперимента допускается только в целях выявления, предупреждения, пресечения и раскрытия тяжкого преступления, а также в целях выявления и установления лиц, их подготавливающих, совершающих или совершивших.
При проведении оперативно-розыскных мероприятий по основаниям, предусмотренным пунктами 1—4 и 6 части второй статьи 7 настоящего Федерального закона, запрещается осуществление действий, указанных в пунктах 8—11 части первой статьи 6 настоящего Федерального закона.
Оперативно-розыскные мероприятия, обеспечивающие безопасность органов, осуществляющих оперативно-розыскную деятельность, проводятся в соответствии с настоящим Федеральным законом и исключительно в пределах полномочий указанных органов, установленных соответствующими законодательными актами Российской Федерации. По основаниям, предусмотренным пунктом 5 части второй статьи 7 настоящего Федерального закона, разрешается осуществлять действия, указанные в пунктах 8—11 части первой статьи 6, без судебного решения при наличии согласия гражданина в письменной форме.

**Статья 9. Основания и порядок судебного рассмотрения материалов об ограничении конституционных прав граждан при проведении оперативно-розыскных мероприятий**

Рассмотрение материалов об ограничении конституционных прав граждан на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, на неприкосновенность жилища при проведении оперативно-розыскных мероприятий осуществляется судом, как правило, по месту проведения таких мероприятий или по месту нахождения органа, ходатайствующего об их проведении. Указанные материалы рассматриваются уполномоченным на то судьей единолично и незамедлительно. Судья не вправе отказать в рассмотрении таких материалов в случае их представления.

Основанием для решения судьей вопроса о проведении оперативно-розыскного мероприятия, ограничивающего конституционные права граждан, указанные в части первой настоящей статьи, является мотивированное постановление одного из руководителей органа, осуществляющего оперативно-розыскную деятельность. Перечень категорий таких руководителей устанавливается ведомственными нормативными актами.

По требованию судьи ему могут представляться также иные материалы, касающиеся оснований для проведения оперативно-розыскного мероприятия, за исключением данных о лицах, внедренных в организованные преступные группы, о штатных негласных сотрудниках органов, осуществляющих оперативно-розыскную деятельность, и о лицах, оказывающих им содействие на конфиденциальной основе, об организации и о тактике проведения оперативно-розыскных мероприятий.

По результатам рассмотрения указанных материалов судья разрешает проведение соответствующего оперативно-розыскного мероприятия, которое ограничивает конституционные права граждан, указанные в части первой настоящей статьи, либо отказывает в его проведении, о чем выносит мотивированное постановление. Постановление, заверенное печатью, выдается инициатору проведения оперативно-розыскного мероприятия одновременно с возвращением представленных им материалов.

Срок действия вынесенного судьей постановления исчисляется в сутках со дня его вынесения и не может превышать шести месяцев, если иное не указано в самом постановлении. При этом течение срока не прерывается. При необходимости продления срока действия постановления судья выносит судебное решение на основании вновь представленных материалов.

В случае, если судья отказал в проведении оперативно-розыскного мероприятия, которое ограничивает конституционные права граждан, указанные в части первой настоящей статьи, орган, осуществляющий оперативно-розыскную деятельность, вправе обратиться по этому **же** вопросу в вышестоящий суд.

Руководители судебных органов создают условия, обеспечивающие защиту сведений, которые содержатся в представляемых судье оперативно-служебных документах.

**Статья 10. Информационное обеспечение и документирование оперативно-розыскной деятельности**

Органы, осуществляющие оперативно-розыскную деятельность, для решения задач, возложенных на них настоящим Федеральным законом, могут создавать и использовать информационные системы, а также заводить дела оперативного учета.

Дела оперативного учета заводятся при наличии оснований, предусмотренных пунктами 1—6 части первой статьи 7 настоящего Федерального закона, в целях собирания и систематизации сведений, проверки и оценки результатов оперативно-розыскной деятельности, а также принятия на их основе соответствующих решений органами, осуществляющими оперативно-розыскную деятельность.

Факт заведения дела оперативного учета не является основанием для ограничения конституционных прав и свобод, а также законных интересов человека и гражданина.
Дело оперативного учета прекращается в случаях решения конкретных задач оперативно-розыскной деятельности, предусмотренных статьей 2 настоящего Федерального закона, а также установления обстоятельств, свидетельствующих об объективной невозможности решения этих задач.
Перечень дел оперативного учета и порядок их ведения определяются нормативными актами органов, осуществляющих оперативно-розыскную деятельность.

**Статья 11. Использование результатов оперативно-розыскной деятельности**

Результаты оперативно-розыскной деятельности могут быть использованы для подготовки и осуществления следственных и судебных действий, проведения оперативно-розыскных мероприятий по выявлению, предупреждению, пресечению и раскрытию преступлений, выявлению и установлению лиц, их подготавливающих, совершающих или совершивших, а также для розыска лиц, скрывшихся от органов дознания, следствия и суда, уклоняющихся от исполнения наказания и без вести пропавших.
Результаты оперативно-розыскной деятельности могут служить поводом и основанием для возбуждения уголовного дела, представляться в орган дознания, следователю или в суд, в производстве которого находится уголовное дело, а также использоваться в доказывании по уголовным делам в соответствии с положениями уголовно-процессуального законодательства Российской Федерации, регламентирующими собирание, проверку и оценку доказательств.
Представление результатов оперативно-розыскной деятельности органу дознания, следователю или в суд осуществляется на основании постановления руководителя органа, осуществляющего оперативно-розыскную деятельность, в порядке, предусмотренном ведомственными нормативными актами.
Результаты оперативно-розыскной деятельности в отношении лиц, перечисленных в пунктах 1—4 и 6 части второй статьи 7 настоящего Федерального закона, учитываются при решении вопроса об их допуске к указанным видам деятельности.

**Статья 12. Защита сведений об органах, осуществляющих оперативно-розыскную деятельность**

Сведения об используемых или использованных при проведении негласных оперативно-розыскных мероприятий силах, средствах, источниках, методах, планах и результатах оперативно-розыскной деятельности, о лицах, внедренных в организованные преступные группы, о штатных негласных сотрудниках органов, осуществляющих оперативно-розыскную деятельность, и о лицах, оказывающих им содействие на конфиденциальной основе, а также об организации и о тактике проведения оперативно-розыскных мероприятий составляют государственную тайну и подлежат рассекречиванию только на основании постановления руководителя органа, осуществляющего оперативно-розыскную деятельность.
Предание гласности сведений о лицах, внедренных в организованные преступные группы, о штатных негласных сотрудниках органов, осуществляющих оперативно-розыскную деятельность, а также о лицах, оказывающих или оказывавших им содействие на конфиденциальной основе, допускается лишь с их согласия в письменной форме и в случаях, предусмотренных федеральными законами.
Судебное решение на право проведения оперативно-розыскного мероприятия и материалы, послужившие основанием для принятия такого решения, хранятся только в органах, осуществляющих оперативно-розыскную деятельность.
Оперативно-служебные документы, отражающие результаты оперативно-

розыскной деятельности, могут быть представлены органу дознания, следователю, судье, другим органам, осуществляющим оперативно-розыскную деятельность, в порядке и случаях, установленных настоящим Федеральным законом.

**Глава III. Органы, осуществляющие оперативно-розыскную деятельность**

**Статья 13. Органы, осуществляющие оперативно-розыскную деятельность**

На территории Российской Федерации право осуществлять оперативно-розыскную деятельность предоставляется оперативным подразделениям:

1. Органов внутренних дел Российской Федерации.
2. Органов Федеральной службы безопасности.
3. Федеральных органов налоговой полиции.

Федеральным законом от 18 июля 1997 г. № 101-ФЗ в пункт 4 части первой статьи 13 настоящего Федерального закона внесены изменения, см. текст пункта в предыдущей редакции.

4. Федеральных органов государственной охраны.

Указом Президента РФ от 19 июня 1996 г. № 938 Главное управление охраны Российской Федерации переименовано в Федеральную службу охраны Российской Федерации.

5. Органов пограничной службы Российской Федерации.
6. Таможенных органов Российской Федерации.
7. Службы внешней разведки Российской Федерации.

Оперативные подразделения органа внешней разведки Министерства обороны Российской Федерации и органа внешней разведки Федерального агентства правительственной связи и информации при Президенте Российской Федерации проводят оперативно-розыскные мероприятия только в целях обеспечения безопасности указанных органов внешней разведки и в случае, если проведение этих мероприятий не затрагивает полномочий органов, указанных в пунктах 1—7 части первой настоящей статьи.

Перечень органов, осуществляющих оперативно-розыскную деятельность, может быть изменен или дополнен только федеральным законом. Руководители указанных органов определяют перечень оперативных подразделений, правомочных осуществлять оперативно-розыскную деятельность, их полномочия, структуру и организацию работы.

Органы, осуществляющие оперативно-розыскную деятельность, решают определенные настоящим федеральным законом задачи исключительно в пределах своих полномочий, установленных соответствующими законодательными актами Российской Федерации.

**Статья 14. Обязанности органов, осуществляющих оперативно-розыскную деятельность**

При решении определенных настоящим Федеральным законом задач оперативно-розыскной деятельности органы, уполномоченные ее осуществлять, обязаны:

1. Принимать в пределах своих полномочий все необходимые меры по защите конституционных прав и свобод человека и гражданина, собственности, а также по обеспечению безопасности общества и государства.
2. Исполнять в пределах своих полномочий поручения в письменной форме органа дознания, следователя, указания прокурора и решения суда о проведении оперативно-розыскных мероприятий по уголовным делам, принятым ими к производству.
3. Выполнять на основе и в порядке, предусмотренных международными договорами Российской Федерации, запросы соответствующих международных правоохранительных организаций, правоохранительных органов и специальных служб иностранных государств.
4. Информировать другие органы, осуществляющие оперативно-розыскную деятельность на территории Российской Федерации, о ставших им известными фактах противоправной деятельности, относящихся к компетенции этих органов, и оказывать этим органам необходимую помощь.

О взаимодействии Пограничных войск и органов внутренних дел в оперативно-розыскной деятельности см. Инструкцию, утвержденную приказом ФПС РФ и МВД РФ от 31 января 1995 г. № 57/42.

5. Соблюдать правила конспирации при осуществлении оперативно-розыскной деятельности.

6. Содействовать обеспечению в порядке, установленном законодательством Российской Федерации безопасности и сохранности имущества своих сотрудников, лиц, оказывающих содействие органам, осуществляющим оперативно-розыскную деятельность, участников уголовного судопроизводства, а также членов семей и близких указанных лиц от преступных посягательств.

**Статья 15. Права органов, осуществляющих оперативно-розыскную деятельность**

При решении задач оперативно-розыскной деятельности органы, уполномоченные ее осуществлять, имеют право:

1. Проводить гласно и негласно оперативно-розыскные мероприятия, перечисленные в статье 6 настоящего Федерального закона, производить при их проведении изъятие, предметов, материалов и сообщений, а также прерывать предоставление услуг связи в случае возникновения непосредственной угрозы жизни и здоровью лица, а также угрозы государственной военной экономической или экологической безопасности Российской Федерации.

2. Устанавливать на безвозмездной либо возмездной основе отношения сотрудничества с лицами, изъявившими согласие оказывать содействие на конфиденциальной основе органам, осуществляющим оперативно-розыскную деятельность.

3. Использовать в ходе проведения оперативно-розыскных мероприятий по договору или устному соглашению служебные помещения, имущество предприятий, учреждений, организаций, воинских частей, а также жилые и нежилые помещения, транспортные средства и иное имущество частных лиц.

4. Использовать в целях конспирации документы, зашифровывающие личность должностных лиц, ведомственную принадлежность предприятий, учреждений, организаций, подразделений, помещений и транспортных средств органов, осуществляющих оперативно-розыскную деятельность, а также личность граждан, оказывающих им содействие на конфиденциальной основе.

5. Создавать в установленном законодательством Российской Федерации порядке предприятия, учреждения, организации и подразделения, необходимые для решения задач, предусмотренных настоящим Федеральным законом.

Законные требования должностных лиц органов, осуществляющих оперативно-розыскную деятельность, обязательны для исполнения физическими и юридическими лицами, к которым такие требования предъявлены.

Неисполнение законных требований должностных лиц органов, осуществляющих оперативно-розыскную деятельность либо воспрепятствование ее законному осуществлению влекут ответственность, предусмотренную законодательством Российской Федерации.

**Статья 16. Социальная и правовая защита должностных лиц органов, осуществляющих оперативно-розыскную деятельность**

О государственной защите должностных лиц органов, осуществляющих оперативно-розыскную деятельность, см. Федеральный закон от 20 апреля 1995 г. № 45-ФЗ.

На должностных лиц органов, осуществляющих оперативно-розыскную деятельность, распространяются гарантии социальной и правовой защиты сотрудников тех органов, в штаты которых указанные лица входят.

Никто не вправе вмешиваться в законные действия должностных лиц и органов, осуществляющих оперативно-розыскную деятельность, за исключением лиц, прямо уполномоченных на то федеральным законом.

Должностное лицо, уполномоченное на осуществление оперативно-розыскной деятельности, в ходе проведения оперативно-розыскных мероприятий подчиняется только непосредственному и прямому начальнику. При получении приказа или указания, противоречащего закону, указанное должностное лицо обязано руководствоваться законом.

При защите жизни и здоровья граждан, их конституционных прав и законных интересов, а также для обеспечения безопасности общества и государства от преступных посягательств допускается вынужденное причинение вреда правоохраняемым интересам должностным лицом органа, осуществляющего оперативно-розыскную деятельность, либо лицом, оказывающим ему содействие, совершаемое при правомерном выполнении указанным лицом своего служебного или общественного долга.

Время выполнения должностными лицами органов, осуществляющих оперативно-розыскную деятельность специальных заданий в организованных преступных группах, а также время их службы в должностях штатных негласных сотрудников указанных органов подлежит зачету в выслугу лет для назначения пенсии в льготном исчислении в порядке, определяемом Правительством Российской Федерации.

Органы государственной власти субъектов Российской Федерации и органы местного самоуправления вправе устанавливать дополнительные виды социальной защиты для должностных лиц органов, осуществляющих оперативно-розыскную деятельность.

## Глава IV. Содействие граждан органам, осуществляющим оперативно-розыскную деятельность

### Статья 17. Содействие граждан органам, осуществляющим оперативно-розыскную деятельность

Отдельные лица могут с их согласия привлекаться к подготовке или проведению оперативно-розыскных мероприятий с сохранением по их желанию конфиденциальности содействия органам, осуществляющим оперативно-розыскную деятельность, в том числе по контракту. Эти лица обязаны сохранять в тайне сведения, ставшие им известными в ходе подготовки или проведения оперативно-розыскных мероприятий, и не вправе предоставлять заведомо ложную информацию указанным органам.

Органы, осуществляющие оперативно-розыскную деятельность, могут заключать контракты с совершеннолетними дееспособными лицами независимо от их гражданства, национальности, пола, имущественного, должностного и социального положения, образования, принадлежности к общественным объединениям, отношения к религии и политических убеждений.

Органам, осуществляющим оперативно-розыскную деятельность, запрещается использовать конфиденциальное содействие по контракту депутатов, судей, прокуроров, адвокатов, священнослужителей и полномочных представителей официально зарегистрированных религиозных объединений.

### Статья 18. Социальная и правовая защита граждан, содействующих органам, осуществляющим оперативно-розыскную деятельность

Лица, содействующие органам, осуществляющим оперативно-розыскную деятельность, находятся под защитой государства.

Государство гарантирует лицам, изъявившим согласие содействовать по контракту органам, осуществляющим оперативно-розыскную деятельность, выполнение своих обязательств, предусмотренных контрактом, в том числе гарантирует правовую защиту, связанную с правомерным выполнением указанными лицами общественного долга или возложенных на них обязанностей.

При возникновении реальной угрозы противоправного посягательства на жизнь, здоровье или имущество отдельных лиц в связи с их содействием органам, осуществляющим оперативно-розыскную деятельность, а равно членов их семей и близких, эти органы обязаны принять необходимые меры по предотвращению противоправных действий, установлению виновных и

привлечению их к ответственности, предусмотренной законодательством Российской Федерации.
Лицо из числа членов преступной группы, совершившее противоправное деяние, не повлекшее тяжких последствий, и привлеченное к сотрудничеству с органом, осуществляющим оперативно-розыскную деятельность, активно способствовавшее раскрытию преступлений, возместившее нанесенный ущерб или иным образом загладившее причиненный вред, освобождается от уголовной ответственности в соответствии с законодательством Российской Федерации.
Лица, сотрудничающие с органами, осуществляющими оперативно-розыскную деятельность, либо оказавшие им помощь в раскрытии преступления или установлении лиц, их совершивших, могут получать вознаграждения и другие выплаты. Полученные указанными лицами суммы вознаграждений и другие выплаты налогами не облагаются и в декларациях о доходах не указываются.
Период сотрудничества граждан по контракту с органами, осуществляющими оперативно-розыскную деятельность в качестве основного рода занятий, включается в трудовой стаж граждан. Указанные лица имеют право на пенсионное обеспечение в соответствии с законодательством Российской Федерации.
В целях обеспечения безопасности лиц, сотрудничающих с органами, осуществляющими оперативно-розыскную деятельность, и членов их семей допускается проведение специальных мероприятий по их защите в порядке, определяемом законодательными и иными нормативными правовыми актами Российской Федерации.
В случае гибели лица, сотрудничающего по контракту с органами, осуществляющими оперативно-розыскную деятельность, в связи с его участием в проведении оперативно-розыскных мероприятий семье пострадавшего и лицам, находящимся на его иждивении, из средств соответствующего бюджета выплачивается единовременное пособие в размере десятилетнего денежного содержания погибшего и в установленном законом порядке назначается пенсия по случаю потери кормильца.
При получении лицом, сотрудничающим по контракту с органами осуществляющими оперативно-розыскную деятельность, травмы, ранения, контузии, увечья, наступивших в связи с его участием в проведении оперативно-розыскных мероприятий и исключающих для него возможность дальнейшего сотрудничества с органами, осуществляющими оперативно-розыскную деятельность, указанному лицу из средств соответствующего бюджета выплачивается единовременное пособие в размере пятилетнего денежного содержания и в установленном законом порядке назначается пенсия по инвалидности.

## Глава V. Финансовое обеспечение оперативно-розыскной деятельности

### Статья 19. Финансовое обеспечение оперативно-розыскной деятельности

Государственным органам, оперативные подразделения которых уполномочены осуществлять оперативно-розыскную деятельность, выделяются из федерального бюджета финансовые средства, которые расходуются в порядке, устанавливаемом руководителями этих органов.
Законодательные и исполнительные органы государственной власти субъектов Российской Федерации вправе самостоятельно за счет собственных бюджетов и внебюджетных целевых фондов увеличивать размер средств, выделяемых органам, осуществляющим оперативно-розыскную деятельность на территории соответствующих субъектов Российской Федерации.
Контроль за расходованием финансовых средств, выделенных на оперативно-розыскную деятельность, осуществляется руководителями государственных органов, в состав которых входят оперативные подразделения, осуществляющие оперативно-розыскную деятельность, а также специально

уполномоченными на то представителями Министерства финансов Российской Федерации.

**Глава VI. Контроль и надзор за оперативно-розыскной деятельностью**

**Статья 20. Контроль за оперативно-розыскной деятельностью**

Контроль за оперативно-розыскной деятельностью осуществляют Президент Российской Федерации, Федеральное Собрание Российской Федерации, Правительство Российской Федерации в пределах полномочий, определяемых Конституцией Российской Федерации, федеральными конституционными законами и федеральными законами.

**Статья 21. Прокурорский надзор за оперативно-розыскной деятельностью**

Надзор за исполнением законов Российской Федерации органами, осуществляющими оперативно-розыскную деятельность, осуществляют Генеральный прокурор Российской Федерации и уполномоченные им прокуроры.

По запросу уполномоченного прокурора в связи с поступившими в прокуратуру материалами, информацией и обращениями граждан о нарушении законов при проведении оперативно-розыскных мероприятий, а также при проверке установленного порядка проведения оперативно-розыскных мероприятий и законности принимаемых при этом решений руководители органа, осуществляющего оперативно-розыскную деятельность, представляют указанному прокурору оперативно-служебные документы, послужившие основанием для проведения этих мероприятий.

О порядке предоставления органами внутренних дел материалов для осуществления прокурорского надзора за исполнением настоящего Закона см. указание Генеральной прокуратуры РФ и МВД РФ от 29 июля 1996 г. № 44/15, 25 июля 1996 г. № 1/12812.

Сведения о лицах, внедренных в организованные преступные группы, и о штатных негласных сотрудниках органов, осуществляющих оперативно-розыскную деятельность, а также о лицах, оказывающих или оказывавших содействие этим органам на конфиденциальной основе, представляются прокурору только с письменного согласия указанных лиц, за исключением случаев, требующих их привлечения к уголовной ответственности. Сведения об организации, о тактике, методах и средствах осуществления оперативно-розыскной деятельности в предмет прокурорского надзора не входят.

Руководители органов прокуратуры создают условия, обеспечивающие защиту сведений, содержащихся в представляемых прокурору оперативно-служебных документах.

Об организации прокурорского надзора за оперативно-розыскной деятельностью см. также Федеральный закон от 17 ноября 1995 г. № 168-ФЗ и приказ Генерального прокурора РФ от 20 мая 1993 г. № 15.

**Статья 22. Ведомственный контроль**

Руководители органов, осуществляющих оперативно-розыскную деятельность, несут персональную ответственность за соблюдение законности при организации и проведении оперативно-розыскных мероприятий.

**Статья 23. Вступление в силу настоящего Федерального закона**

Настоящий Федеральный закон вступает в силу со дня его официального опубликования.

Признать утратившим силу со дня введения в действие настоящего Федерального закона Закон Российской Федерации «Об оперативно-розыскной деятельности в Российской Федерации» (Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации, 1992, № 17, ст. 892; № 33, ст. 1912).

Предложить Президенту Российской Федерации и поручить Правительству Российской Федерации привести их нормативные правовые акты в соответствие с настоящим Федеральным законом.

**Москва, Кремль**

**12 августа 1995 г.**
**Президент Российской Федерации Б. Ельцин**
**«О МЕРАХ ПО РЕАЛИЗАЦИИ ПРАВОВОЙ ИНФОРМАТИЗАЦИИ» Указ Президента РФ от 28 июня 1993 г. № 963**
В целях ускорения работ по правовой информатизации России ПОСТАНОВЛЯЮ:
1. Возложить на научно-технический центр правовой информации «Система» Федерального агентства правительственной связи и информации при Президенте Российской Федерации функции головной организации по реализации правовой информатизации России.
2. Для осуществления задач по организации и ведению эталонного банка данных правовой информации, необходимого для формирования правовой политики, реализации программ законопроектных работ и правового обеспечения проводимых в Российской Федерации реформ, а также осуществления координации деятельности предприятий, организаций и учреждений, участвующих в реализации концепции правовой информатизации России, ввести должность генерального конструктора правовой информатизации России.
3. Утвердить генеральным конструктором правовой информатизации России Киселева Бориса Валентиновича.
4. Установить, что генеральный конструктор правовой информатизации России по должности входит в состав коллегии Федерального агентства правительственной связи и информации при Президенте Российской Федерации. Государственно-правовому управлению Президента Российской Федерации как генеральному заказчику по созданию систем правовой информатизации в двухнедельный срок определить круг полномочий и порядок деятельности генерального конструктора правовой информатизации России.
Установить должностной оклад, а также условия материально-бытового обеспечения генерального конструктора правовой информатизации России на уровне первого заместителя Генерального директора Федерального агентства правительственной связи и информации при Президенте Российской Федерации.
5. Федеральному агентству правительственной связи и информации при Президенте Российской Федерации осуществлять организационно-техническое обеспечение деятельности генерального конструктора правовой информатизации России.
**28 июня 1993 г.**
**Президент Российской Федерации Б. Ельцин**
**«ОБ ОБРАЗОВАНИИ ФЕДЕРАЛЬНОЙ КОМИССИИ ПО ПРАВОВОЙ ИНФОРМАТИЗАЦИИ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ» Указ Президента РФ от 28 января 1994 г. № 223**
В целях активизации процесса создания государственной системы правовой информатизации России и обеспечения реализации Указа Президента Российской Федерации от 28 июня 1993 г. № 966 «О Концепции правовой информатизации России»
ПОСТАНОВЛЯЮ:
1. Образовать Федеральную, комиссию по правовой информатизации при Президенте Российской Федерации (далее именуется — Комиссия).
2. Утвердить председателем Комиссии начальника Государственно-правового управления Президента Российской Федерации **Орехова Руслана Геннадьевича.**
3. Включить в состав Комиссии:
**Маслова Александра Васильевича** — начальника отдела Государственно-правового управления Президента Российской Федерации (заместитель председателя Комиссии);
**Антипова Владимира Серафимовича** — начальника отдела Главного управления охраны Российской Федерации;

**Караваева Николая Алексеевича** — начальника управления Генеральной прокуратуры Российской Федерации (по согласованию);
**Киселева Бориса Валентиновича** — генерального конструктора правовой информатизации Российской Федерации;
**Кузьмина Владимира Максимовича —** первого заместителя Министра юстиции Российской Федерации;
**Левченко Владимира Александровича** — первого заместителя начальника Управления информационных ресурсов Администрации Президента Российской Федерации;
**Некрасова Владимира Ивановича** — консультанта Государственно-правового управления Президента Российской Федерации (ответственный секретарь Комиссии);
**Окунькова Льва Андреевича —** директора Института законодательства и сравнительного правоведения при Правительстве Российской Федерации;
**Радченко Владимира Ивановича** — первого заместителя Председателя Верховного Суда Российской Федерации (по согласованию);
**Старовойтова Александра Владимировича** — генерального директора Федерального агентства правительственной связи и информации при Президенте Российской Федерации;
**Топорнина Бориса Николаевича** — директора Института государства и права Российской академии наук;
**Цыганенке Игоря Григорьевича** — заведующего юридическим отделом Аппарата Правительства Российской Федерации;
**Юкова Михаила Кузьмича** — первого заместителя Председателя Высшего Арбитражного Суда Российской Федерации (по согласованию).
4. Утвердить Положение о Федеральной комиссии по правовой информатизации при Президенте Российской Федерации (прилагается).
**Москва, Кремль**
**28 января 1994 г.**
**Президент Российской Федерации Б. Ельцин**
**ПОЛОЖЕНИЕ**
**О Федеральной комиссии по правовой информатизации при Президенте Российской Федерации**
**I. Общие положения**
1. Федеральная комиссия по правовой информатизации при Президенте Российской Федерации (далее именуется — Комиссия) является постоянно действующим совещательным и консультативным органом при Президенте Российской Федерации, обеспечивающим разработку комплекса мер по созданию и функционированию государственной системы правовой информатизации, формированию единого информационно-правового пространства России, обеспечивающего правовую информированность государственных органов, общественных и других организаций, граждан. В своей деятельности Комиссия подотчетна Президенту Российской Федерации.
Комиссия осуществляет свои полномочия во взаимодействии с органами государственной власти Российской Федерации, органами исполнительной власти республик в составе Российской Федерации, краев, областей, автономной области, автономных округов, городов Москвы и Санкт-Петербурга.
2. Комиссия в своей деятельности руководствуется Конституцией Российской Федерации, законами и иными нормативными актами Российской Федерации, указами и распоряжениями Президента Российской Федерации, постановлениями Правительства Российской Федерации, а также настоящим Положением.
**II. Задачи Комиссии**
3. Основными задачами Комиссии являются:
>• разработка предложений по формированию стратегии государственной политики в области правовой информатизации России;

>• подготовка федеральной программы правовой информатизации России;
>• подготовка и представление Президенту Российской Федерации и Правительству Российской Федерации проектов нормативных актов по вопросам правовой информатизации и правового обеспечения информационных процессов и информатизации;
>• выработка предложений по координации работ в области разработки;
>• внедрения и развития государственной системы правовой информатизации России, систематизации законодательства, подготовке Свода законов Российской Федерации и Свода актов Президента и Правительства Российской Федерации;
>• взаимодействие с компетентными органами Содружества Независимых Государств и международными организациями по вопросам создания и функционирования межгосударственной системы правовой информатизации.

**III. Полномочия Комиссии**

4. Комиссия для решения стоящих перед ней задач:
>• готовит заключения по поступающим на подпись Президенту Российской Федерации законам по вопросам правовой информации, информатизации и защиты информации;
>• рассматривает проекты указов и распоряжений Президента Российской Федерации, постановлений и распоряжений Правительства Российской Федерации по вопросам правовой информатизации и правового обеспечения информационных процессов и информатизации и готовит по ним заключения;
**>•** дает рекомендации по реализации решений Президента Российской Федерации (по его поручениям) по вопросам правовой информатизации;
**>•** осуществляет оценку состояния дел по информационно-правовому обеспечению деятельности органов исполнительной власти Российской Федерации, а также организует проверки выполнения указов и распоряжений Президента Российской Федерации, постановлений и распоряжений Правительства Российской Федерации, касающихся вопросов правовой информатизации;
>• в соответствии со своей компетенцией запрашивает у органов государственной власти и управления необходимые для осуществления деятельности Комиссии информацию, документы и материалы;
**>•** привлекает к своей работе представителей министерств, ведомств, правоохранительных органов, специалистов научно-исследовательских организаций.

5. Решения Комиссии по вопросам правовой информатизации реализуются указами и распоряжениями Президента Российской Федерации, постановлениями и распоряжениями Правительства Российской Федерации.

**IV. Организация деятельности Комиссии**

6. Состав Комиссии, включая ее председателя, утверждается Президентом Российской Федерации.
Работа членов Комиссии осуществляется на безвозмездной основе.
7. Заседания Комиссии проводятся по мере необходимости, но не реже одного раза в месяц в соответствии с планом работы Комиссии.
Решения на заседаниях принимаются большинством голосов присутствующих членов комиссии.
8. Для проработки вопросов подготовки заседаний, проведения экспертных работ Комиссия может создавать рабочие группы.

**V. Обеспечение деятельности Комиссии**

9. Организационно-техническое обеспечение деятельности Комиссии осуществляется соответствующими структурными подразделениями Администрации Президента Российской Федерации.
10. Информационно-правовое обеспечение деятельности Комиссии осуществляется Государственно-правовым управлением Президента Российской Федерации, являющимся рабочим аппаратом Комиссии.

**«О МЕРАХ ПО СОБЛЮДЕНИЮ ЗАКОННОСТИ В ОБЛАСТИ РАЗРАБОТКИ ПРОИЗВОДСТВА,**

**РЕАЛИЗАЦИИ И ЭКСПЛУАТАЦИИ ШИФРОВАЛЬНЫХ СРЕДСТВ, А ТАКЖЕ ПРЕДОСТАВЛЕНИЯ УСЛУГ В ОБЛАСТИ ШИФРОВАНИЯ ИНФОРМАЦИИ»**

**Указ Президента РФ от 3 апреля 1995 г. № 334**

В целях обеспечения безусловного исполнения Закона Российской Федерации «О федеральных органах правительственной связи и информации, а также усиления борьбы с организованной преступностью и повышения защищенности информационно-телекоммуникационных систем органов государственной власти, российских кредитно-финансовых структур, предприятий и организаций ПОСТАНОВЛЯЮ:

1. Придать Программе создания и развития информационно-телекоммуникационной системы специального назначения в интересах органов государственной власти статус президентской программы. Центру президентских программ Администрации Президента Российской Федерации совместно с Федеральным агентством правительственной связи и информации при Президенте Российской Федерации обеспечить ее доработку и реализацию.
2. Запретить использование государственными организациями и предприятиями в информационно-телекоммуникационных системах шифровальных средств, включая криптографические средства обеспечения подлинности информации (электронная подпись), и защищенных технических средств хранения, обработки и передачи информации, не имеющих сертификата Федерального агентства правительственной связи и информации при Президенте Российской Федерации, а также размещение государственных заказов на предприятиях, в организациях, использующих указанные технические и шифровальные средства, не имеющие сертификата Федерального агентства правительственной связи и информации при Президенте Российской Федерации.
3. Предложить Центральному банку Российской Федерации и Федеральному агентству правительственной связи и информации при Президенте Российской Федерации принять необходимые меры в отношении коммерческих банков Российской Федерации, уклоняющихся от обязательного использования, имеющих сертификат Федерального агентства правительственной связи и информации при Президенте Российской Федерации защищенных технических средств хранения, обработки и передачи информации при их информационном взаимодействии с подразделениями Центрального банка Российской Федерации.
4. В интересах информационной безопасности Российской Федерации и усиления борьбы с организованной преступностью запретить деятельность юридических и физических лиц, связанную с разработкой, производством, реализацией и эксплуатацией шифровальных средств, а также защищенных технических средств хранения, обработки и передачи информации, предоставлением услуг в области шифрования информации, без лицензий, выданных Федеральным агентством правительственной связи и информации при Президенте Российской Федерации в соответствии с Законом Российской Федерации «О федеральных органах правительственной связи и информации».
5. Государственному таможенному комитету Российской Федерации принять меры к недопущению ввоза на территорию Российской Федерации шифровальных средств иностранного производства без лицензии Министерства внешних экономических связей Российской Федерации, выданной по согласованию с Федеральным агентством правительственной связи и информации при Президенте Российской Федерации.
6. Федеральной службе контрразведки Российской Федерации и Министерству внутренних дел Российской Федерации совместно с Федеральным агентством правительственной связи и информации при Президенте Российской Федерации, Государственной налоговой службой Российской Федерации и Департаментом налоговой полиции Российской Федерации осуществлять выявление юридических и физических лиц, нарушающих требования

настоящего Указа.
7. Предложить Генеральной прокуратуре Российской Федерации усилить прокурорский надзор за соблюдением Закона Российской Федерации «О федеральных органах правительственной связи и информации» в части разработки производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации в Российской Федерации, подлежащих лицензированию и сертификации Федеральным агентством правительственной связи и информации при Президенте Российской Федерации.
8. Создать Федеральный центр защиты экономической информации при Федеральном агентстве правительственной связи и информации при Президенте Российской Федерации (в пределах штатной численности этого Агентства), возложив на него разработку и реализацию комплексных программ обеспечения безопасности экономической информации российских кредитно-финансовых и других экономически значимых структур страны.
9. Генеральному директору Федерального агентства правительственной связи и информации при Президенте Российской Федерации в 2-месячный срок утвердить положение об указанном центре.
10. Настоящий Указ вступает в силу со дня его опубликования.

**Москва, Кремль**
**3 апреля 1995 г.**
**Президент Российской Федерации Б. Ельцин**

**«ПОЛОЖЕНИЕ**
**О ГОСУДАРСТВЕННОЙ ТЕХНИЧЕСКОЙ КОМИССИИ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»**
**Указ Президента РФ от 19 февраля 1999 г. № 212**
**Выписка**

В соответствии со статьей 32 Федерального конституционного закона «О Правительстве Российской Федерации» постановляю:
1. Утвердить прилагаемое Положение о Государственной технической комиссии при Президенте Российской Федерации.
2. Утвердить перечень руководящих работников федеральных органов исполнительной власти, государственных органов и организаций Российской Федерации, которые входят в состав коллегии Государственной технической комиссии при Президенте Российской Федерации по должности, согласно приложению № 1.
3. Для служебного пользования.
4. Правительству Российской Федерации в месячный срок утвердить состав коллегии Государственной технической комиссии при Президенте Российской Федерации (далее именуется — Гостехкомиссия России).
См. состав коллегии Государственной технической комиссии при Президенте Российской Федерации, утвержденный распоряжением Правительства РФ от 10 апреля 1999 г. NQ 565-р.
5. Утвердить предельную штатную численность центрального аппарата Гостехкомиссии России в количестве 163 единиц (без персонала по охране и обслуживанию зданий).
Установить фонд оплаты труда работников центрального аппарата Гостехкомиссии России в размере 5117,2 тыс. рублей.
Разрешить прикомандирование к Гостехкомиссии России в пределах установленной штатной численности до 136 военнослужащих.
6. Создать при Гостехкомиссии России в соответствии с федеральными законами «Об обороне» и «О воинской обязанности и военной службе» инженерно-технические воинские формирования, включив в их состав головную научную организацию по проблемам защиты информации от технических разведок и от ее утечки по техническим каналам и региональные центры, образованные на базе специальных центров Министерства обороны Российской Федерации и головной научной

организации, подчиненных Гостехкомиссии России в специальном отношении, исключив их из состава Вооруженных Сил Российской Федерации.
7. Для служебного пользования.
8. Разрешить иметь в Гостехкомиссии России четырех заместителей председателя Государственной технической комиссии при Президенте Российской Федерации, в том числе двух первых заместителей председателя Государственной технической комиссии при Президенте Российской Федерации и одного статс-секретаря — заместителя председателя Государственной технической комиссии при Президенте Российской Федерации.
9. Сохранить существующие порядок размещения и обеспечения деятельности центрального аппарата Гостехкомиссии России и инженерно-технических воинских формирований при Гостехкомиссии России, порядок материального, продовольственного, вещевого и пенсионного обеспечения, бытового, медицинского и санаторно-курортного обслуживания военнослужащих, обеспечения их жильем, а также льготы и компенсации военнослужащим и членам их семей.
10. Осуществлять финансирование расходов на содержание центрального аппарата Гостехкомиссии России и инженерно-технических воинских формирований при Гостехкомиссии России за счет средств федерального бюджета, в том числе расходов на содержание центрального аппарата Гостехкомиссии России — за счет средств федерального бюджета, предусмотренных на государственное управление.
11. Признать утратившими силу:
>• Указ Президента Российской Федерации от 5 января 1992 г. № 9 «О создании Государственной технической комиссии при Президенте Российской Федерации» (Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР, 1992, № 3, ст. 109);
>• Указ Президента Российской Федерации от 6 июня 1996 г. № 815 «О численности работников центрального аппарата Государственной технической комиссии при Президенте Российской Федерации» (Собрание законодательства Российской Федерации, 1996, № 24, ст. 2873);
>• распоряжение Президента Российской Федерации от 28 декабря 1992 г. № 829-рпс;
>• распоряжение Президента Российской Федерации от 5 июля 1993 г. № 483-рпс.
12. Настоящий Указ вступает в силу со дня его официального опубликования.

**Москва, Кремль**
**19 февраля 1999 г.**
**Президент Российской Федерации Б. Ельцин**

**ПОЛОЖЕНИЕ**

**О Государственной технической комиссии при Президенте Российской Федерации Утверждено Указом Президента РФ от 19 февраля 1999 г. № 212**

**I. Общие положения**

1. Государственная техническая комиссия при Президенте Российской Федерации (далее именуется — Гостехкомиссия России) является федеральным органом исполнительной власти, осуществляющим межотраслевую координацию и функциональное регулирование деятельности по обеспечению защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную или служебную тайну, от ее утечки по техническим каналам, от несанкционированного доступа к ней, от специальных воздействий на информацию в целях ее уничтожения, искажения и блокирования и по противодействию техническим средствам разведки на территории Российской Федерации (далее именуется — техническая защита информации), а также единую государственную научно-техническую политику в области защиты информации при разработке, производстве, эксплуатации

и утилизации неинформационных излучающих комплексов, систем и устройств.
Гостехкомиссия России организует деятельность государственной системы защиты информации в Российской Федерации от технических разведок и от ее утечки по техническим каналам.
Гостехкомиссия России и региональные центры входят в состав государственных органов обеспечения безопасности Российской Федерации.
2. Гостехкомиссия России в своей деятельности руководствуется Конституцией Российской Федерации, федеральными конституционными законами, федеральными законами, указами и распоряжениями Президента Российской Федерации, постановлениями и распоряжениями Правительства Российской Федерации, международными договорами Российской Федерации, а также настоящим Положением.
3. Президент Российской Федерации в соответствии с Конституцией Российской Федерации, федеральными конституционными законами, федеральными законами руководит деятельностью Гостехкомиссии России.
4. Правительство Российской Федерации в соответствии с Конституцией Российской Федерации, федеральными конституционными законами, федеральными законами координирует деятельность Гостехкомиссии России.
5. Приказы, распоряжения и указания Гостехкомиссии России, изданные в пределах ее компетенции, обязательны для исполнения аппаратами федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, органами местного самоуправления, предприятиями, учреждениями и организациями.
6. Гостехкомиссия России осуществляет свою деятельность во взаимодействии с другими федеральными органами исполнительной власти, государственными органами, предприятиями, учреждениями и организациями.
7. Членами коллегии Гостехкомиссии России по должности являются руководящие работники федеральных органов исполнительной власти, государственных органов и организаций Российской Федерации в соответствии с перечнем, утверждаемым Президентом Российской Федерации.
Состав коллегии Гостехкомиссии России утверждается Правительством Российской Федерации.
8. На заседания (совещания) коллегии Гостехкомиссии России выносятся наиболее важные вопросы, имеющие межведомственный характер.
9. Деятельность Гостехкомиссии России обеспечивают ее центральный аппарат, инженерно-технические воинские формирования при Гостехкомиссии России, в состав которых входят головная научная организация по проблемам защиты информации от технических разведок и от ее утечки по техническим каналам (далее именуется — головная научная организация) и региональные центры.
10. По решению Президента Российской Федерации при Гостехкомиссии России могут создаваться подведомственные организации.
11. Гостехкомиссия России является в пределах своих полномочий государственным заказчиком по проведению общесистемных научных исследований в области технической защиты информации, а также по разработке и производству технических средств защиты информации общего применения и средств контроля эффективности этой защиты.
Средства на финансирование указанных работ выделяются Гостехкомиссии России из федерального бюджета.
12. Гостехкомиссия России, инженерно-технические воинские формирования при Гостехкомиссии России являются юридическими лицами, имеют действительные и условные наименования, печати с изображением Государственного герба Российской Федерации и со своими наименованиями, расчетные и иные счета, включая валютные, в банках и других кредитных

организациях.

**II. Основные задачи Гостехкомиссии России**

13. Основными задачами Гостехкомиссии России являются:

>• проведение единой государственной политики в области технической защиты информации;

>• осуществление единой государственной научно-технической политики в области защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;

>• осуществление межотраслевой координации и функционального регулирования деятельности по обеспечению технической защиты информации в аппаратах органов государственной власти Российской Федерации и органов государственной власти субъектов Российской Федерации, федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации, органах местного самоуправления, на предприятиях, в учреждениях и организациях;

>• прогнозирование развития сил, средств и возможностей технических разведок, выявление угроз безопасности информации;

>• противодействие добыванию информации техническими средствами разведки, предотвращение утечки информации по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию в целях ее уничтожения, искажения и блокирования;

>• контроль в пределах своих полномочий деятельности по технической защите информации в аппаратах федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации, органах местного самоуправления, на предприятиях, в учреждениях и организациях;

>• осуществление организационно-технического обеспечения деятельности Межведомственной комиссии по защите государственной тайны центральным аппаратом Гостехкомиссии России.

**III. Функции и полномочия Гостехкомиссии России**

14. Гостехкомиссия России осуществляет следующие функции:

**>•** формирует общую стратегию и определяет приоритетные направления технической защиты информации;

>• осуществляет на плановой основе межотраслевую координацию деятельности по обеспечению технической защиты информации в аппаратах федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации, органах местного самоуправления, на предприятиях, в учреждениях и организациях;

>• организует и финансирует изучение излучений различной физической природы, возникающих при использовании неинформационных излучающих комплексов, систем и устройств;

**>•** определяет основные направления научных исследований в области технической защиты информации;

>• утверждает нормативно-методические документы по технической защите информации (концепции, положения, требования, нормы, модели, методики, рекомендации и другие) и организует их издание за счет средств, выделяемых Гостехкомиссии России на эти цели;

>• координирует деятельность федеральных органов исполнительной власти по организации системы технической защиты информации от утечки при использовании неинформационных излучающих комплексов, систем и устройств; организует изучение влияния неинформационных излучающих комплексов, систем и устройств на организм человека и окружающую среду;

**>•** осуществляет лицензирование деятельности по разработке, производству, эксплуатации и утилизации неинформационных излучающих

комплексов, систем и устройств, а также их сертификацию;
>• выполняет в установленном порядке специальные работы по технической защите информации;
>• осуществляет методическое руководство в области технической защиты информации в отношении аппаратов федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления, предприятий, учреждений и организаций;
>• участвует в разработке и проведении мероприятий по технической защите информации в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации;
>• участвует в согласовании проектов решений по составу экспортных комплектаций оборудования и документации при поставках на экспорт продукции военного назначения;
>• принимает участие в решении вопросов организации технической защиты информации в процессе осуществления военно-технического сотрудничества Российской Федерации с иностранными государствами;
>• разрабатывает предложения по развитию научной, экспериментальной и производственной базы для технической защиты информации, руководит головной научной организацией, организует проведение научно-исследовательских и опытно-конструкторских работ в области технической защиты информации;
>• разрабатывает и согласовывает программу стандартизации и проекты государственных стандартов в области технической защиты информации;
>• разрабатывает и согласовывает в установленном порядке федеральные целевые программы по обеспечению технической защиты информации;
>• рассматривает по поручениям Президента Российской Федерации и Правительства Российской Федерации проекты нормативных правовых актов в области технической защиты информации;
**>•** участвует в согласовании вопросов размещения на территории Российской Федерации дипломатических и консульских учреждений иностранных государств;
**>•** разрабатывает и представляет в Правительство Российской Федерации согласованные с заинтересованными федеральными органами исполнительной власти и органами исполнительной власти субъектов Российской Федерации предложения о внесении изменений в перечень территорий Российской Федерации с регламентированным посещением для иностранных граждан;
>• проводит работу по прогнозированию развития сил, средств и возможностей технических разведок, по оценке их осведомленности о сведениях, составляющих государственную тайну, и формирует банк данных по этим вопросам, а также определяет порядок доступа к указанным данным заинтересованных федеральных органов исполнительной власти;
**>•** осуществляет лицензирование деятельности, связанной с оказанием услуг в области технической защиты информации, созданием средств технической защиты информации, а также средств технического контроля эффективности защиты информации;
>• участвует совместно с Федеральной службой безопасности Российской Федерации в проведении на договорной основе специальных экспертиз по допуску предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, а также в государственной аттестации руководителей предприятий, учреждений и организаций, ответственных за защиту сведений, составляющих государственную тайну;
>• осуществляет работы по сертификации средств технической защиты информации;
>• рассматривает (разрабатывает) предложения к переговорным позициям

государственных делегаций Российской Федерации с целью обеспечения условий по технической защите информации;
>• осуществляет методическое обеспечение работ по технической защите информации в ходе подготовки и реализации международных договоров (соглашений) по укреплению мер доверия, сокращению (ограничению) вооруженных сил и вооружений, при функционировании на территории Российской Федерации предприятий с иностранными инвестициями, а также при введении режимов открытости;
>• осуществляет методическое руководство деятельностью органов исполнительной власти субъектов Российской Федерации по созданию региональных систем технической защиты информации;
>• осуществляет методическое руководство подготовкой, профессиональной переподготовкой и повышением квалификации специалистов в области технической защиты информации;
>• осуществляет в пределах своих полномочий контроль за состоянием работ по технической защите информации в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации, органах местного самоуправления, на предприятиях, в учреждениях и организациях;
>• организует проведение радиоконтроля за соблюдением установленного порядка передачи служебных сообщений должностными лицами предприятий, учреждений и организаций, выполняющими работы, связанные со сведениями, составляющими государственную или служебную тайну, при использовании открытых каналов радио- и радиорелейных, тропосферных и спутниковых линий связи, доступных для радиоразведки;
>• осуществляет международное сотрудничество в пределах своих полномочий.
15. Гостехкомиссия России имеет право:
>• представлять Президенту Российской Федерации, в Правительство Российской Федерации и Совет Безопасности Российской Федерации предложения по нормативному правовому регулированию в области технической защиты информации;
>• вносить в Правительство Российской Федерации согласованные с заинтересованными федеральными органами исполнительной власти и органами исполнительной власти субъектов Российской Федерации предложения о внесении изменений в перечень территорий Российской Федерации с регламентированным посещением для иностранных граждан;
>• вносить в государственные органы представления о применении установленных законодательством Российской Федерации мер ответственности за нарушения в области технической защиты информации;
>• проводить работы с использованием активных средств противодействия техническим разведкам;
>• осуществлять контроль за соблюдением федерального законодательства о технической защите информации и требований руководящих и нормативно-методических документов Гостехкомиссии России предприятиями, учреждениями и организациями, имеющими лицензии Гостехкомиссии России;
>• осуществлять контроль деятельности по технической защите информации в аппаратах федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации, органах местного самоуправления, на предприятиях, в учреждениях и организациях (в Министерстве обороны Российской Федерации, Службе внешней разведки Российской Федерации, Федеральной службе безопасности Российской Федерации, Федеральной службе охраны Российской Федерации, Федеральной пограничной службе Российской Федерации, Федеральном агентстве правительственной связи и информации при Президенте Российской Федерации и Главном управлении специальных

программ Президента Российской Федерации — по согласованию с руководителями указанных органов);

>• контролировать с применением технических средств эффективность защиты государственных и промышленных объектов, образцов вооружения и военной техники при их разработке, производстве и полигонных испытаниях (по согласованию с Генеральным штабом Вооруженных Сил Российской Федерации), информационных систем, средств и систем связи и управления (в отношении технических средств и систем Министерства обороны Российской Федерации, Службы внешней разведки Российской Федерации, Федеральной службы безопасности Российской Федерации, Федеральной службы охраны Российской Федерации, Федеральной пограничной службы Российской Федерации, Федерального агентства правительственной связи и информации при Президенте Российской Федерации и Главного управления специальных программ Президента Российской Федерации, а также объектов и технических средств органов государственной власти Российской Федерации, защита которых входит в их компетенцию, — по согласованию с соответствующими руководителями);

,>• выдавать предписания на приостановление работ на объектах федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления, предприятий, учреждений и организаций в случае выявления в ходе проведения контроля нарушений норм и требований, касающихся технической защиты информации;

>• заслушивать на заседаниях коллегии Гостехкомиссии России должностных лиц, ответственных за организацию технической защиты информации в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации, органах местного самоуправления, на предприятиях, в учреждениях и организациях;

>• утверждать квалификационные требования к специалистам в области технической защиты информации и согласовывать учебные программы подготовки, профессиональной переподготовки и повышения квалификации специалистов в области технической защиты информации;

>• организовывать и проводить семинары, конференции и симпозиумы, в том числе международные, по вопросам технической защиты информации.

**IV. Руководство Гостехкомиссии России**

16. Гостехкомиссию России возглавляет председатель Государственной технической комиссии при Президенте Российской Федерации, назначаемый на должность и освобождаемый от должности Президентом Российской Федерации.

Председатель Гостехкомиссии России в ходе осуществления межотраслевой координации деятельности по технической защите информации пользуется правами федерального министра.

17. Председатель Гостехкомиссии России имеет четырех заместителей, в том числе двух первых заместителей и одного статс-секретаря — заместителя председателя Гостехкомиссии России, назначаемых на должность и освобождаемых от должности Президентом Российской Федерации по представлению председателя Гостехкомиссии России.

18. Председатель Гостехкомиссии России:

>• организует работу Гостехкомиссии России, осуществляет руководство инженерно-техническими воинскими формированиями при Гостехкомиссии России;

>• несет персональную ответственность за выполнение возложенных на Гостехкомиссию России задач;

>• распределяет обязанности между своими заместителями, определяет полномочия и задачи других должностных лиц;

>• издает приказы и распоряжения в пределах своих полномочий;

>• утверждает положения о подразделениях Гостехкомиссии России,

входящих в ее структуру;
>• заключает, возобновляет, изменяет, расторгает трудовые договоры (контракты) с сотрудниками Гостехкомиссии России в соответствии с федеральным законодательством;
>• представляет Гостехкомиссию России во взаимоотношениях с федеральными органами государственной власти, иными государственными органами и организациями;
>• издает в установленном порядке нормативные правовые акты по вопросам технической защиты информации;
>• вносит в установленном порядке на рассмотрение Президента Российской Федерации и в Правительство Российской Федерации проекты нормативных правовых актов и предложения о совершенствовании федерального законодательства, касающиеся технической защиты информации;
>• издает в установленном порядке нормативные правовые акты, регулирующие деятельность Гостехкомиссии России и инженерно-технических воинских формирований при Гостехкомиссии России, обеспечивает их исполнение;
>• утверждает в пределах установленных численности и фонда оплаты труда работников штатное расписание Гостехкомиссии России, а также смету на ее содержание в пределах средств, выделенных из федерального бюджета на соответствующий год;
>• утверждает положение о региональных центрах, а также устав головной научной организации;
>• утверждает в пределах установленной численности структуру и штатное расписание инженерно-технических воинских формирований при Гостехкомиссии России;
**>•** зачисляет в установленном порядке граждан Российской Федерации на военную службу в инженерно-технические воинские формирования при Гостехкомиссии России;
>• пользуется в отношении военнослужащих инженерно-технических воинских формирований при Гостехкомиссии России правами, предусмотренными Дисциплинарным уставом Вооруженных Сил Российской Федерации, в полном объеме;
>• утверждает в установленном порядке смету внебюджетных средств;
**>•** вносит в установленном порядке предложения об изменении штатной численности Гостехкомиссии России и инженерно-технических воинских формирований при Гостехкомиссии России, а также о структуре Гостехкомиссии России;
>• представляет на утверждение Президента Российской Федерации общее количество воинских должностей в инженерно-технических воинских формированиях при Гостехкомиссии России, подлежащих замещению полковниками (капитанами 1 ранга);
>• присваивает военнослужащим инженерно-технических воинских формирований при Гостехкомиссии России воинские звания до полковника (капитана 1 ранга) включительно;
>• осуществляет в пределах своей компетенции назначение на должность и освобождение от должности лиц командного состава инженерно-технических воинских формирований при Гостехкомиссии России; в пределах своей компетенции увольняет военнослужащих инженерно-технических воинских формирований при Гостехкомиссии России с военной службы в запас либо в отставку, а также приостанавливает их военную службу в установленном федеральным законодательством порядке;
>• определяет порядок зачета военнослужащим инженерно-технических воинских формирований при Гостехкомиссии России стажа их трудовой деятельности до зачисления на военную службу в выслугу лет для назначения пенсии;
**>•** принимает в соответствии с федеральными законами и иными

нормативными правовыми актами Российской Федерации решения о продлении срока военной службы отдельным военнослужащим инженерно-технических воинских формирований при Гостехкомиссии России из числа квалифицированных специалистов, достигшим предельного возраста пребывания на военной службе;

>• определяет порядок обеспечения денежным довольствием военнослужащих инженерно-технических воинских формирований при Гостехкомиссии России, а также условия и систему оплаты труда гражданского персонала в соответствии с федеральным законодательством;

>• определяет порядок и условия выплаты сотрудникам Гостехкомиссии России, военнослужащим и гражданскому персоналу инженерно-технических воинских формирований при Гостехкомиссии России доплат, надбавок, премий и других вознаграждений, предусмотренных законодательством Российской Федерации;

>• вносит на рассмотрение Президента Российской Федерации представления о награждении государственными наградами Российской Федерации сотрудников Гостехкомиссии России, военнослужащих и гражданского персонала инженерно-технических воинских формирований при Гостехкомиссии России, а также других лиц, оказывающих содействие в решении возложенных на Гостехкомиссию России задач, и о присвоении им почетных званий;

>• учреждает ведомственные награды (медали и нагрудные знаки) для награждения сотрудников Гостехкомиссии России, военнослужащих и гражданского персонала инженерно-технических воинских формирований при Гостехкомиссии России, а также других лиц, оказывающих содействие в решении возложенных на Гостехкомиссию России задач;

>• имеет наградной и подарочный фонды, в том числе огнестрельного и холодного оружия, для награждения сотрудников Гостехкомиссии России, военнослужащих и гражданского персонала инженерно-технических воинских формирований при Гостехкомиссии России, а также других лиц, оказывающих содействие в решении возложенных на Гостехкомиссию России задач;

**>•** награждает именным огнестрельным и холодным оружием в порядке, установленном федеральным законодательством, а также ведомственными наградами, ценными подарками или деньгами;

>• заключает с командирами инженерно-технических воинских формирований при Гостехкомиссии России контракты о прохождении военной службы в соответствии с федеральным законодательством;

>• представляет руководителям федеральных органов исполнительной власти предложения о прикомандировании военнослужащих к центральному аппарату Гостехкомиссии России;

>• возбуждает ходатайства о продлении сроков военной службы отдельным военнослужащим, прикомандированным к Гостехкомиссии России, по достижении ими предельного возраста пребывания на военной службе;

>• представляет в Правительство Российской Федерации проект бюджетной заявки на выделение Гостехкомиссии России средств из федерального бюджета;

**>•** утверждает смету расходов на содержание центрального аппарата Гостехкомиссии России и инженерно-технических воинских формирований при Гостехкомиссии России в пределах средств, выделяемых из федерального бюджета на соответствующий год;

>• распоряжается финансовыми средствами Гостехкомиссии России, является распорядителем кредитов в пределах средств, выделяемых из федерального бюджета на содержание Гостехкомиссии России, включая валютные средства;

>• заключает на конкурсной основе договоры с научными организациями на выполнение научно-исследовательских и опытно-конструкторских работ в области технической защиты информации;

>• вносит в установленном порядке представления о применении мер

ответственности за нарушения требований федерального законодательства о технической защите информации;
>• запрашивает и получает от федеральных органов исполнительной власти, иных государственных органов, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления, предприятий, учреждений и организаций, должностных лиц необходимые для осуществления деятельности Гостехкомиссии России информацию, документы и материалы, в том числе добытые по специальным каналам;
>• принимает решения о проведении внеочередных заседаний (совещаний) коллегии Гостехкомиссии России;
>• создает межведомственные рабочие и экспертные группы, привлекает ведущих специалистов различного профиля, в том числе на договорной основе, к осуществлению аналитических и экспертных работ по технической защите информации;
>• подписывает в установленном порядке международные договоры Российской Федерации;
>• решает в установленном порядке вопросы, связанные с приемом в Гостехкомиссии России иностранных делегаций (представителей) и командированием делегаций (сотрудников) Гостехкомиссии России;
в иностранные государства;
>• принимает в соответствии с федеральным законодательством решения о выезде за пределы Российской Федерации сотрудников Гостехкомиссии России, военнослужащих и гражданского персонала инженерно-технических воинских формирований при Гостехкомиссии России.

**V. Порядок работы коллегии Гостехкомиссии России**

19. Заседания (совещания) коллегии Гостехкомиссии России проводятся не реже одного раза в квартал. В случае необходимости по инициативе председателя Гостехкомиссии России могут проводиться ее внеочередные заседания (совещания).
Присутствие на заседании (совещании) коллегии Гостехкомиссии России ее членов обязательно. Они не вправе делегировать свои полномочия иным лицам. В случае отсутствия члена коллегии Гостехкомиссии России на заседании (совещании) он вправе изложить свое мнение по рассматриваемым вопросам в письменном виде.
20. Члены коллегии Гостехкомиссии России обладают равными правами при обсуждении рассматриваемых на ее заседании (совещании) вопросов.
Решения коллегии Гостехкомиссии России принимаются большинством голосов присутствующих на заседании (совещании) членов коллегии Гостехкомиссии России-Решения коллегии Гостехкомиссии России при необходимости оформляются приказом Гостехкомиссии России, подписываемым ее председателем.
Протоколы заседаний (совещаний) коллегии Гостехкомиссии России подписываются председательствующим на заседании (совещании).
В случае несогласия с принятым решением члены коллегии Гостехкомиссии России вправе изложить в письменном виде свое мнение, которое подлежит приобщению к протоколу заседания (совещания). В этом случае председатель докладывает о возникших разногласиях Президенту Российской Федерации. Члены коллегии также могут сообщить свое мнение Президенту Российской Федерации.
21. Подготовка материалов к заседанию (совещанию) коллегии Гостехкомиссии России осуществляется ее центральным аппаратом и представителями тех федеральных органов исполнительной власти, к ведению которых относятся вопросы повестки дня.
22. В случае необходимости для участия в заседаниях (совещаниях) коллегии Гостехкомиссии России могут приглашаться представители федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, руководители предприятий,

учреждений и организаций.

**Приложение № 1 к Указу Президента РФ от 19 февраля 1999 г. № 212**

ПЕРЕЧЕНЬ руководящих работников федеральных органов исполнительной власти, государственных органов и организаций Российской Федерации, которые входят в состав коллегии Государственной технической комиссии при Президенте Российской Федерации, по должности

Первый заместитель Министра Российской Федерации по атомной энергии

Первый заместитель Министра внутренних дел Российской Федерации

Первый заместитель Министра Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий

Заместитель Министра иностранных дел Российской Федерации

Первый заместитель Министра науки и технологий Российской Федерации

Заместитель Министра экономики Российской Федерации

Заместитель Министра юстиции Российской Федерации

Заместитель председателя Госкомэкологии России

Первый заместитель председателя Госкомсвязи России

Первый заместитель директора ФСБ России

Заместитель руководителя ФСО России

Заместитель директора СВР России

Первый заместитель генерального директора ФАПСИ

Начальник вооружения Вооруженных Сил Российской Федерации

Начальник Главного оперативного управления Генерального штаба Вооруженных Сил Российской Федерации — первый заместитель начальника Генерального штаба Вооруженных Сил Российской Федерации

Первый заместитель начальника ГУСПа

Заместитель Председателя Банка России Вице-президент Российской академии наук

**«О ЛИЦЕНЗИРОВАНИИ ОТДЕЛЬНЫХ ВИДОВ ДЕЯТЕЛЬНОСТИ» Постановление Правительства РФ от 11 апреля 2000 г. № 326**

**Правительство Российской Федерации** ПОСТАНОВЛЯЕТ:

1. Утвердить прилагаемый перечень федеральных органов исполнительной власти, осуществляющих лицензирование.

2. Установить, что полномочия федеральных органов исполнительной власти по лицензированию конкретных видов деятельности определяются в постановлениях Правительства Российской Федерации, утверждающих положения о лицензировании этих видов деятельности, если иное не установлено соответствующими федеральными законами, вступающими в силу со дня вступления в силу Федерального закона «О лицензировании отдельных видов деятельности», и указами Президента Российской Федерации.

3. Федеральным органам исполнительной власти по перечню, указанному в пункте 1 настоящего постановления, представить в установленном порядке во II квартале 2000 г. в Правительство Российской Федерации проекты положений о лицензировании соответствующих видов деятельности с учетом пункта 2 настоящего постановления и пункта 3 статьи 19 Федерального закона «О лицензировании отдельных видов деятельности».

4. Утвердить прилагаемый перечень видов деятельности, лицензирование которых осуществляется органами исполнительной власти субъектов Российской Федерации, и федеральных органов исполнительной власти, разрабатывающих проекты положений о лицензировании этих видов деятельности.

5. Федеральным органам исполнительной власти по перечню, указанному в пункте 4 настоящего постановления, разработать с участием органов государственной власти субъектов Российской Федерации и представить в установленном порядке во II квартале 2000 г. в Правительство Российской Федерации проекты положений о лицензировании соответствующих видов

деятельности, осуществляемом органами исполнительной власти субъектов Российской Федерации.

6. Возложить на Министерство экономики Российской Федерации методическое руководство разработкой федеральными органами исполнительной власти проектов положений о лицензировании конкретных видов деятельности.

7. Федеральным органам исполнительной власти, включенным в перечни, утвержденные настоящим постановлением, при внесении в Правительство Российской Федерации проектов положений о лицензировании конкретных видов деятельности представлять при необходимости в установленном порядке и предложения о признании утратившими силу или приведении в соответствие с Федеральным законом закона «О лицензировании отдельных видов деятельности» принятых ранее нормативных правовых актов.

8. Признать утратившим силу постановление Правительства Российской Федерации от 24 декабря 1994 г. № 1418 «О лицензировании отдельных видов деятельности», кроме предпоследнего абзаца пункта 5 и абзацев первого и второго пункта 8 Порядка ведения лицензионной деятельности, утвержденного указанным постановлением (Собрание законодательства Российской Федерации, 1995, № 1, ст. 69; № 24, ст. 2280; № 33, ст. 3394; № 43, ст. 4062; 1997, № 17, ст. 2011; № 49, ст. 5601).

**Председатель Правительства Российской Федерации В. Путин**

**ПЕРЕЧЕНЬ**

**федеральных органов исполнительной власти, осуществляющих лицензирование**

**МВД России**

Деятельность в области пожарной безопасности.

Изготовление, установка и эксплуатация технических средств и систем регулирования дорожного движения.

Торговля оружием, его приобретение, коллекционирование или экспонирование (за исключением приобретения оружия государственными военизированными организациями).

Деятельность по охране драгоценных металлов и драгоценных камней при проведении операций с указанными ценностями.

Осуществление частной охранной деятельности.

Осуществление частной сыскной деятельности.

Создание объединений частных детективных предприятий.

Использование объектов и помещений, где осуществляется деятельность, связанная с оборотом наркотических средств и психотропных веществ.

**<• • •>**

Госстандарт России и иные федеральные органы исполнительной власти, на которые законодательными актами Российской Федерации возлагаются организация и проведение работ по обязательной сертификации.

Деятельность центров обязательной сертификации.

Деятельность испытательных лабораторий (экспертных центров) в области обязательной сертификации.

**<• • •>**

**ФСБ России**

Разработка и производство специальных технических средств, предназначенных для негласного получения информации.

Реализация специальных технических средств, предназначенных для Приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации.

**ФСБ России, СВР России**

Деятельность предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну.

**ФСБ России, ФАПСИ, Гостехкомиссия России, СВР России**

Проведение работ, связанных с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны.

**ФСБ России, ФАПСИ, СВР России**

Деятельность по использованию технических средств, предназначенных для выявления электронных устройств, служащих для негласного получения информации.

**<• • •>**

**ФАПСИ**

Деятельность по распространению шифровальных средств. Деятельность по техническому обслуживанию шифровальных средств Предоставление услуг в области шифрования информации. Формирование федеральных информационных ресурсов и (или) информационных ресурсов совместного ведения на основе договора.

Осуществление права удостоверения идентичности электронной цифровой подписи.

**<• • •>**

**Гостехкомиссия России, ФАПСИ, Минфин России**

Деятельность по производству специальных защитных знаков, предназначенных для маркирования товаров, сопроводительной документации к товарам и подтверждения подлинности документов и ценных бумаг.

Деятельность по распространению специальных защитных знаков, предназначенных для маркирования товаров, сопроводительной документации к товарам и подтверждения подлинности документов и пенных бумаг.

**Гостехкомиссия России, ФАПСИ, Минобороны России, СВР России**

Проведение работ, связанных с созданием средств защиты информации, составляющие государственную тайну.

**Гостехкомиссия России, ФАПСИ**

Проектирование средств защиты информации и обработки персональных данных.

Производство средств защиты информации и обработки персональных данных.

**<• • •>**

**«О ЛИЦЕНЗИРОВАНИИ ОТДЕЛЬНЫХ ВИДОВ ДЕЯТЕЛЬНОСТИ» Постановление Правительства РФ от 24 декабря 1994 г. № 1418 (с изменениями, внесенными Постановлением Правительства РФ от 11 апреля 2000 г. № 326 г.)**

В целях проведения единой государственной политики в области лицензирования отдельных видов деятельности и обеспечения защиты жизненно важных интересов личности, общества и государства Правительство Российской Федерации

ПОСТАНОВЛЯЕТ:

**<• • •>**

5. Федеральные органы исполнительной власти, иные специально уполномоченные на ведение лицензионной деятельности органы, указанные в приложений 1 к настоящему постановлению, органы исполнительной власти субъектов Российской Федерации осуществляют лицензионную деятельность на основании положений о лицензировании отдельных видов деятельности, утверждаемых Правительством Российской Федерации. В положениях о лицензировании отдельных видов деятельности федеральным органам исполнительной власти и иным специально уполномоченным на ведение лицензионной деятельности органам, указанным в приложении 1 к настоящему постановлению, может быть предоставлено право передачи полномочий по лицензированию соответствующих видов деятельности органам исполнительной власти субъектов Российской Федерации.

**<• • •>**

**Председатель Правительства Российской Федерации В. Черномырдин**

**Порядок ведения лицензионной деятельности <• • •>**

8. Деятельность на основании лицензии, выданной органами исполнительной

власти субъектов Российской Федерации, на территории иных субъектов Российской Федерации может осуществляться после регистрации таких лицензий органами исполнительной власти соответствующих субъектов Российской Федерации. Регистрация проводится в течение 30 дней по предъявлении оригинала лицензии с проверкой, при необходимости, указанных в лицензии данных, условий осуществления соответствующего вида деятельности и условий безопасности. О проведенной регистрации в лицензии делается отметка о занесении в реестр выданных, зарегистрированных, приостановленных и аннулированных лицензий.

**<• • •>**

**«О ЛИЦЕНЗИРОВАНИИ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЙ, УЧРЕЖДЕНИЙ И ОРГАНИЗАЦИЙ ПО ПРОВЕДЕНИЮ РАБОТ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ ГОСУДАРСТВЕННУЮ ТАЙНУ, СОЗДАНИЕМ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ, А ТАКЖЕ С ОСУЩЕСТВЛЕНИЕМ МЕРОПРИЯТИЙ И (ИЛИ) ОКАЗАНИЕМ УСЛУГ ПО ЗАЩИТЕ ГОСУДАРСТВЕННОЙ ТАЙНЫ»**

**Постановление Правительства РФ от 15 апреля 1995 г. № 333 (с изменениями от 23 апреля 1996 г., 30 апреля 1997 г., 29 июля 1998 г.)**

В соответствии с Законом Российской Федерации «О государственной тайне» и в целях установления порядка допуска предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны. Правительство Российской Федерации

ПОСТАНОВЛЯЕТ:

1. Утвердить Положение о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны (прилагается).
2. Установить, что размер платы за рассмотрение заявлений о выдаче лицензий на проведение работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны, составляет 10 минимальных размеров оплаты труда. Суммы, полученные от рассмотрения заявления и выдачи лицензии, поступают в федеральный бюджет, за счет средств которого содержится орган, уполномоченный на ведение лицензионной деятельности.
3. Федеральной службе безопасности Российской Федерации, Государственной технической комиссии при Президенте Российской Федерации, федеральному агентству правительственной связи и информации при Президенте Российской Федерации, Службе внешней разведки Российской Федерации совместно с заинтересованными министерствами и ведомствами Российской Федерации в 3-месячный срок разработать комплекс мер организационного, материально-технического и иного характера, необходимых для осуществления лицензирования деятельности предприятий, организаций и учреждений по проведению работ, связанных с использованием сведений, составляющих государственную тайну.
4. Установить, что предприятия, учреждения и организации, допущенные к моменту принятия настоящего постановления к работам, связанным с использованием сведений, составляющих государственную тайну, могут осуществлять эти работы в течение 1995 года.

**Председатель Правительства Российской Федерации В. Черномырдин**

**ПОЛОЖЕНИЕ**

**О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих**

**государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны Утверждено постановлением Правительства РФ от 15 апреля 1995 г. № 333 с изменениями от 23 апреля 1996 г., 30 апреля 1997 г., 29 июля 1998 г.**

1. Настоящее Положение устанавливает порядок лицензирования деятельности предприятий, учреждений и организаций независимо от их организационно-правовых форм (далее именуются — предприятия) по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны. Лицензия является официальным документом, который разрешает осуществление на определенных условиях конкретного вида деятельности в течение установленного срока. Лицензия действительна на всей территории Российской Федерации, а также в учреждениях Российской Федерации, находящихся за границей.

2. Органами, уполномоченными на ведение лицензионной деятельности, являются:

>• по допуску предприятий к проведению работ, связанных с использованием сведений, составляющих государственную тайну, — Федеральная служба безопасности Российской Федерации и ее территориальные органы (на территории Российской Федерации), Служба внешней разведки Российской Федерации (за рубежом);

(Постановлением Правительства РФ от 29 июля 1998 г. № 854 в абзац третий пункта 2 настоящего Положения были внесены изменения, см. текст абзаца в предыдущей редакции.)

>• на право проведения работ, связанных с созданием средств защиты информации, — Государственная техническая комиссия при Президенте Российской Федерации, Федеральное агентство правительственной связи и информации при Президенте Российской Федерации, Служба внешней разведки Российской Федерации, Министерство обороны Российской Федерации, Федеральная служба безопасности Российской Федерации (в пределах их компетенции);

>» на право осуществления мероприятий и (или) оказания услуг в области защиты государственной тайны — Федеральная служба безопасности Российской Федерации и ее территориальные органы, Федеральное агентство правительственной связи и информации при Президенте Российской Федерации, Государственная техническая комиссия при Президенте Российской Федерации, Служба внешней разведки Российской Федерации (в пределах их компетенции).

Лицензирование деятельности предприятий Федеральной службы безопасности Российской Федерации, Министерства обороны Российской Федерации, Федерального агентства правительственной связи и информации при Президенте Российской Федерации, Федеральной пограничной службы Российской Федерации, Службы внешней разведки Российской Федерации, Государственной технической комиссии при Президенте Российской Федерации по допуску к проведению работ, связанных с использованием сведений, составляющих государственную тайну, осуществляется руководителями министерств и ведомств Российской Федерации, которым подчинены указанные предприятия.

3. На орган, уполномоченный на ведение лицензионной деятельности, возлагается:

>• организация лицензирования деятельности предприятий;

>• организация и проведение специальных экспертиз предприятий;

**>•** рассмотрение заявлений предприятий о выдаче лицензий;

>• принятие решений о выдаче или об отказе в выдаче лицензий;

>• выдача лицензий;

>• принятие решений о приостановлении действия лицензии или о ее аннулировании;
>• разработка нормативно-методических документов по вопросам лицензирования;
>• привлечение в случае необходимости представителей министерств и ведомств Российской Федерации для проведения специальных экспертиз;
>• ведение реестра выданных, приостановленных и аннулированных лицензий.
4. Работа органов, уполномоченных на ведение лицензионной деятельности, координируется Межведомственной комиссией по защите государственной тайны (далее именуется — Межведомственная комиссия)(СМ.Сноску 1).
5. Для получения лицензии заявитель представляет в соответствующий орган, уполномоченный на ведение лицензионной деятельности:
а) заявление о выдаче лицензии с указанием:
>• наименования и организационно-правовой формы, юридического адреса предприятия, номера его расчетного счета в банке;
>• вида деятельности, на осуществление которого должна быть выдана лицензия;
>• срока действия лицензии;
б) копии учредительных документов (с предъявлением оригиналов, в случае если копии не заверены нотариусом);
в) копию свидетельства о государственной регистрации предприятия;
г) копии документов, подтверждающих право собственности, право полного хозяйственного ведения и (или) договора аренды на имущество, необходимое для ведения заявленного вида деятельности;
д) справку о постановке на учет в налоговом органе;
е) документ, подтверждающий оплату рассмотрения заявления. Заявитель несет ответственность за достоверность представляемых им сведений. Все документы, представленные для получения лицензии, регистрируются органом, уполномоченным на ведение лицензионной деятельности.
6. Орган, уполномоченный на ведение лицензионной деятельности, принимает решение о выдаче или об отказе в выдаче лицензии в течение 30 дней со дня получения заявления со всеми необходимыми документами.
В случае необходимости проведения дополнительной экспертизы предприятия решение принимается в 15-дневный срок после получения заключения экспертизы, но не позднее чем через 60 дней со дня подачи заявления о выдаче лицензии и необходимых для этого документов.

___
Сноска 1. Функции Межведомственной комиссии в соответствии с Указом Президента Российской Федерации от 30 марта 1994 г. № 614 временно возложены на Государственную техническую комиссию при Президенте Российской Федерации. Указ Президента РФ от 30 марта 1994 г. № 614 утратил силу. Указом Президента РФ от 20 января 1996 г. № 71 утверждены состав и структура Межведомственной комиссии по защите государственной тайны.
В зависимости от сложности и объема подлежащих специальной экспертизе материалов руководитель органа, уполномоченного на ведение лицензионной деятельности, может продлить срок принятия решения о выдаче или об отказе в выдаче лицензии до 30 дней.
7. Лицензии выдаются на основании результатов специальных экспертиз предприятий и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих государственную тайну (далее именуются — руководители предприятий), и при выполнении следующих условий:
>• соблюдение требований законодательных и иных нормативных актов Российской Федерации по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ, связанных с

использованием указанных сведений; наличие в структуре предприятия подразделения по защите государственной тайны и необходимого числа специально подготовленных сотрудников для работы по защите информации, уровень квалификации которых достаточен для обеспечения защиты государственной тайны;

>• наличие на предприятии средств защиты информации, имеющих сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

8. В лицензии указываются:

>• наименование органа, ее выдавшего;

>• наименование и юридический адрес предприятия, ее получившего;

>• вид деятельности, на осуществление которого выдана лицензия;

>• условия осуществления данного вида деятельности;

>• срок действия лицензии;

>• ее регистрационный номер и дата выдачи.

Срок действия лицензии устанавливается в зависимости от специфики вида деятельности, но не может быть менее трех и более пяти лет.

По просьбе заявителя лицензии могут выдаваться на срок менее трех лет. Продление срока действия лицензии производится в порядке, установленном для ее получения. На каждый вид деятельности выдается отдельная лицензия. В случае если лицензируемый вид деятельности осуществляется на нескольких территориально обособленных объектах, лицензиату одновременно с лицензией выдаются заверенные копии с указанием местоположения каждого объекта. Копии лицензий регистрируются органом, уполномоченным на ведение лицензионной деятельности. Предприятие может иметь лицензии на несколько видов деятельности. Лицензии оформляются на бланках, имеющих степень защиты, соответствующую степени защиты ценной бумаги на предъявителя. Бланки лицензий являются документами строгой отчетности, имеют учетную серию и номер. Приобретение, учет и хранение бланков лицензий возлагается на органы, уполномоченные на ведение лицензионной деятельности. Лицензия выдается после представления заявителем документа, подтверждающего ее оплату, размер которой равен стоимости бланка лицензии.

Лицензия подписывается руководителем (заместителем руководителя) органа, уполномоченного на ведение лицензионной деятельности, и заверяется печатью этого органа. Копия лицензии хранится в органе, уполномоченном на ведение лицензионной деятельности. Передача лицензии другому юридическому лицу запрещена. В случае реорганизации предприятия, получившего лицензию, изменения его местонахождения или наименования, утраты им лицензии оно обязано в 15-дневный срок подать заявление о переоформлении лицензии.

Переоформление лицензии производится в порядке, установленном для ее получения.

До переоформления лицензии лицензиат осуществляет деятельность на основании ранее выданной лицензии или временного разрешения, выдаваемого органом, уполномоченным на ведение лицензионной деятельности, в случае утраты лицензии.

9. Орган, уполномоченный на ведение лицензионной деятельности, вправе отказать в выдаче лицензии. Письменное уведомление об отказе в выдаче лицензии с указанием причин отказа направляется заявителю в 3-дневный срок после принятия соответствующего решения.

Основанием для отказа в выдаче лицензии является:

>• наличие в документах, представленных заявителем, недостоверной или искаженной информации;

>• отрицательное заключение экспертизы, установившей несоответствие необходимым для осуществления заявленного вида деятельности условиям, указанным в пункте 7 настоящего Положения;

>• отрицательное заключение по результатам государственной аттестации руководителя предприятия.

10. Специальная экспертиза предприятия проводится путем проверки выполнения требований нормативно-методических документов по режиму секретности, противодействию иностранным техническим разведкам и защите информации от утечки по техническим каналам, а также соблюдения других условий, необходимых для получения лицензии.

Постановлением Правительства РФ от 30 апреля 1997 г. № 513 абзац второй пункта 10 настоящего Положения после слов: «Служба внешней разведки Российской Федерации» дополнен словами: «Министерство обороны Российской Федерации».

Государственными органами, ответственными за организацию и проведение специальных экспертиз предприятий, являются Федеральная служба безопасности Российской Федерации, Федеральное агентство правительственной связи и информации при Президенте Российской Федерации, Государственная техническая комиссия при Президенте Российской Федерации, Служба внешней разведки Российской Федерации, другие министерства и ведомства Российской Федерации, руководители которых наделены полномочиями по отнесению к государственной тайне сведений в отношении подведомственных им предприятий.

Организация и порядок проведения специальных экспертиз предприятий определяются инструкциями, которые разрабатываются указанными государственными органами и согласовываются с Межведомственной комиссией.

Для проведения специальных экспертиз эти государственные органы могут создавать аттестационные центры, которые получают лицензии в соответствии с требованиями настоящего Положения.

Постановлением Правительства РФ от 30 апреля 1997 г. № 513 абзац пятый пункта 10 настоящего Положения после слов: «Служба внешней разведки Российской Федерации» дополнен словами: «Министерство обороны Российской Федерации».

Специальные экспертизы аттестационных центров проводят Федеральная служба безопасности Российской Федерации, Федеральное агентство правительственной связи и информации при Президенте Российской Федерации, Государственная техническая комиссия при Президенте Российской Федерации, Служба внешней разведки Российской Федерации и их органы на местах (в пределах их компетенции).

Специальные экспертизы проводятся на основе договора между предприятием и органом, проводящим специальную экспертизу. Расходы по проведению специальных экспертиз относятся на счет предприятия.

11. Государственная аттестация руководителей предприятий организуется органами, уполномоченными на ведение лицензионной деятельности, а также министерствами и ведомствами Российской Федерации, руководители которых наделены полномочиями по отнесению к государственной тайне сведений в отношении подведомственных им предприятий. Методические рекомендации по организации и проведению государственной аттестации руководителей предприятий разрабатываются Межведомственной комиссией. Расходы по государственной аттестации руководителей предприятий относятся на счет предприятий. От государственной аттестации освобождаются руководители предприятий, имеющие свидетельство об окончании учебных заведений, уполномоченных осуществлять подготовку специалистов по вопросам защиты информации, составляющей государственную тайну. Перечень указанных учебных заведений утверждается Межведомственной комиссией по представлению органов, уполномоченных на ведение лицензионной деятельности.

12. Органы, уполномоченные на ведение лицензионной деятельности, приостанавливают действие лицензии или аннулируют ее в случае:

>• предоставления лицензиатом соответствующего заявления;
>• обнаружения недостоверных данных в документах, представленных для получения лицензии;
>• нарушения лицензиатом условий действия лицензии;
**>•** невыполнения лицензиатом предписаний или распоряжений государственных органов "или приостановления этими государственными органами деятельности предприятия в соответствии с законодательством Российской Федерации;
>• ликвидации предприятия.
Решение о приостановлении, возобновлении и аннулировании лицензии принимается органом, выдавшим лицензию.
Орган, уполномоченный на ведение лицензионной деятельности, в 3-дневный срок со дня принятия решения о приостановлении действия лицензии или о ее аннулировании в письменной форме уведомляет об этом лицензиата и органы Государственной налоговой службы Российской Федерации. Действие лицензии приостанавливается со дня получения лицензиатом указанного уведомления.
После уведомления владельца лицензии о ее аннулировании, она подлежит возврату в 10-дневяый срок в орган, ее выдавший.
В случае изменения обстоятельств, повлекших приостановление действия лицензии, действие лицензии может быть возобновлено.
Лицензия считается возобновленной после принятия органом, уполномоченным на ведение лицензионной деятельности, соответствующего решения, о котором не позднее чем в 3-дневный срок с момента принятия он оповещает лицензиата и органы Государственной налоговой службы Российской Федерации.
13. Органы, уполномоченные на ведение лицензионной деятельности, ежеквартально представляют в Межведомственную комиссию сведения о выданных и аннулированных лицензиях.
14. Контроль за соблюдением лицензионных условий лицензиатами, выполняющими работы, связанные с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны осуществляют органы, уполномоченные на ведение лицензионной деятельности.
15. Руководители и должностные лица органов, уполномоченных на ведение лицензионной деятельности, несут ответственность за нарушение или ненадлежащее исполнение настоящего Положения в соответствии с законодательством Российской Федерации.
16. Решения и действия органов, уполномоченных на ведение лицензионной деятельности, могут быть обжалованы в установленном порядке.

**«О СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ» Постановление Правительства РФ от 26 июня 1995 г. № 608 (в ред. Постановления Правительства РФ от 23 апреля 1996 г. № 509)**

В соответствии с Законами Российской Федерации «О государственной тайне» и «О сертификации продукции и услуг» Правительство Российской Федерации
ПОСТАНОВЛЯЕТ:
1. Утвердить прилагаемое Положение о сертификации средств защиты информации.
2. Государственной технической комиссии при Президенте Российской Федерации, Федеральному агентству правительственной связи и информации при Президенте Российской Федерации, Федеральной службе безопасности Российской Федерации и Министерству обороны Российской Федерации в пределах определенной законодательством Российской Федерации компетенции в 3-месячный срок разработать и ввести в действие соответствующие положения о системах сертификации, перечни средств

защиты информации, подлежащих сертификации в конкретной системе сертификации, а также по согласованию с Министерством финансов Российской Федерации порядок оплаты работ по сертификации средств защиты информации.

**Председатель Правительства Российской Федерации В. Черномырдин**

**ПОЛОЖЕНИЕ**

**О сертификации средств защиты информации (в ред. Постановления Правительства РФ от 23 апреля 1996 г. № 509)**

1. Настоящее Положение устанавливает порядок сертификации средств защиты информации в Российской Федерации и ее учреждениях за рубежом. Технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации являются средствами защиты информации.

Указанные средства подлежат обязательной сертификации, которая проводится в рамках систем сертификации средств защиты информации.

Система сертификации средств защиты информации представляет собой совокупность участников сертификации, осуществляющих ее по установленным правилам (далее именуется — система сертификации).

Системы сертификации создаются Государственной технической комиссией при Президенте Российской Федерации, Федеральным агентством правительственной связи и информации при Президенте Российской Федерации, Федеральной службой безопасности Российской Федерации, Министерством обороны Российской Федерации, Службой внешней разведки Российской Федерации, уполномоченными проводить работы по сертификации средств защиты информации в пределах компетенции, определенной для них законодательными и иными нормативными актами Российской Федерации (далее именуются — федеральные органы по сертификации). (В ред. Постановления Правительства РФ от 23 апреля 1996 г. № 509.)

Сертификация средств защиты информации осуществляется на основании требований государственных стандартов, нормативных документов, утверждаемых Правительством Российской Федерации и федеральными органами по сертификации в пределах их компетенции.

Координацию работ по организации сертификации средств защиты информации осуществляет Межведомственная комиссия по защите государственной тайны (далее именуется — Межведомственная комиссия)(СМ.сноску 1).

В каждой системе сертификации разрабатываются и согласовываются с Межведомственной комиссией положение об этой системе сертификации, а также перечень средств защиты информации, подлежащих сертификации, и требования, которым эти средства должны удовлетворять.

2. Участниками сертификации средств защиты информации являются:

>• федеральный орган по сертификации;

>• центральный орган системы сертификации (создаваемый при необходимости) — орган, возглавляющий систему сертификации однородной продукции;

>• органы по сертификации средств защиты информации — органы, проводящие сертификацию определенной продукции;

>• испытательные лаборатории — лаборатории, проводящие сертификационные испытания (отдельные виды этих испытаний) определенной продукции;

>• изготовители — продавцы, исполнители продукции.

Центральные органы системы сертификации, органы по сертификации средств защиты информации и испытательные лаборатории проводят аккредитацию на право проведения работ по сертификации, в ходе которой федеральные органы по сертификации определяют возможности выполнения этими органами и лабораториями работ по сертификации средств защиты информации и оформляют официальное разрешение на право проведения

___

Сноска 1. Функции Межведомственной комиссии по защите государственной тайны в соответствии с Указом Президента Российской Федерации от 30 марта 1994 г. № 614 временно возложены на Государственную техническую комиссию при Президенте Российской Федерации.

___

указанных работ. Аккредитация проводится только при наличии у указанных органов и лабораторий лицензии на соответствующие виды деятельности.

3. Федеральный орган по сертификации в пределах своей компетенции:

>• создает системы сертификации;

>• осуществляет выбор способа подтверждения соответствия средств защиты информации требованиям нормативных документов;

**>•** устанавливает правила аккредитации центральных органов систем сертификации, органов по сертификации средств защиты информации и испытательных лабораторий;

>• определяет центральный орган для каждой системы сертификации;

>• выдает сертификаты и лицензии на применение знака соответствия;

>• осуществляет государственные контроль и надзор за соблюдением участниками сертификации правил сертификации и за сертифицированными средствами защиты информации, а также устанавливает порядок инспекционного контроля;

>• рассматривает апелляции по вопросам сертификации;

>• представляет на государственную регистрацию в Комитет Российской Федерации по стандартизации, метрологии и сертификации системы сертификации и знак соответствия;

>• устанавливает порядок признания зарубежных сертификатов;

>• приостанавливает или отменяет действие выданных сертификатов.

4. Центральный орган системы сертификации:

**>•** организует работы по формированию системы сертификации и руководство ею, координирует деятельность органов по сертификации средств защиты информации и испытательных лабораторий, входящих в систему сертификации;

>• ведет учет входящих в систему сертификации органов по сертификации средств защиты информации и испытательных лабораторий, выданных и аннулированных сертификатов и лицензий на применение знака соответствия;

>• обеспечивает участников сертификации информацией о деятельности системы сертификации.

При отсутствии в системе сертификации центрального органа его функции выполняются федеральным органом по сертификации.

5. Органы по сертификации средств защиты информации:

>• сертифицируют средства защиты информации, выдают сертификаты и лицензии на применение знака соответствия с представлением копий в федеральные органы по сертификации и ведут их учет;

**>•** приостанавливают либо отменяют действие выданных ими сертификатов и лицензий на применение знака соответствия;

>• принимают решение о проведении повторной сертификации при изменениях в технологии изготовления и конструкции (составе) сертифицированных средств защиты информации;

>• формируют фонд нормативных документов, необходимых для сертификации;

>• представляют изготовителям по их требованию необходимую информацию в пределах своей компетенции.

6. Испытательные лаборатории проводят сертификационные испытания средств защиты информации и по их результатам оформляют заключения и протоколы, которые направляют в соответствующий орган по сертификации средств защиты информации и изготовителям.

Испытательные лаборатории несут ответственность за полноту испытаний средств защиты информации и достоверность их результатов.

7. Изготовители:
>• производят (реализуют) средства защиты информации только при наличии сертификата;
>• извещают орган по сертификации, проводивший сертификацию, об изменениях в технологии изготовления и конструкции (составе) сертифицированный средств защиты информации;
>• маркируют сертифицированные средства защиты информации знаком соответствия в порядке, установленном для данной системы сертификации;
>• указывают в сопроводительной технической документации сведения о сертификации и нормативных документах, которым средства защиты информации должны соответствовать, а также обеспечивают доведение этой информации до потребителя;
>• применяют сертификат и знак соответствия, руководствуясь законодательством Российской Федерации и правилами, установленными для данной системы сертификации;
>• обеспечивают соответствие средств защиты информации требованиям нормативных документов по защите информации;
>• обеспечивают беспрепятственное выполнение своих полномочий должностными лицами органов, осуществляющих сертификацию, и контроль за сертифицированными средствами защиты информации;
>• прекращают реализацию средств защиты информации при несоответствии их требованиям нормативных документов или по истечении срока действия сертификата, а также в случае приостановки действия сертификата или его отмены.
Изготовители должны иметь лицензию на соответствующий вид деятельности.
8. Изготовитель для получения сертификата направляет в орган по сертификации средств защиты информации заявку на проведение сертификации, к которой могут быть приложены схема проведения сертификации, государственные стандарты и иные нормативные и методические документы, требованиям которых должны соответствовать сертифицируемые средства защиты информации.
Орган по сертификации средств защиты информации в месячный срок после получения заявки направляет изготовителю решение о проведении сертификации с указанием схемы ее проведения, испытательной лаборатории, осуществляющей испытания средств защиты информации, и нормативных документов, требованиям которых должны соответствовать сертифицируемые средства защиты информации, а при необходимости — решение о проведении и сроках предварительной проверки производства средств защиты информации.
Для признания зарубежного сертификата изготовитель направляет его копию и заявку на признание сертификата в федеральный орган по сертификации, который извещает изготовителя о признании сертификата или необходимости проведения сертификационных испытаний в срок не позднее одного месяца после получения указанных документов. В случае признания зарубежного сертификата федеральный орган по сертификации оформляет и выдает изготовителю сертификат соответствия установленного образца.
Сертификация импортируемых средств защиты информации проводится по тем же правилам, что и отечественных.
Основными схемами проведения сертификации средств защиты информации являются:
>• для единичных образцов средств защиты информации — проведение испытаний этих образцов на соответствие требованиям по защите информации;
>• для серийного производства средств защиты информации — проведение типовых испытаний образцов средств защиты информации на соответствие требованиям по защите информации и последующий инспекционный контроль за стабильностью характеристик сертифицированных средств защиты

информации, определяющих выполнение этих требований. Кроме того, допускается предварительная проверка производства по специально разработанной программе. Срок действия сертификата не может превышать пяти лет. 9. Испытания сертифицируемых средств защиты информации проводятся на образцах, технология изготовления и конструкция (состав) которых должны соответствовать образцам, поставляемым потребителю (заказчику).

В отдельных случаях по согласованию с органом по сертификации средств защиты информации допускается проведение испытаний на испытательной базе изготовителя. При этом орган по сертификации средств защиты информации определяет условия, необходимые для обеспечения объективности результатов испытаний.

В случае отсутствия к началу проведения сертификации аккредитованных испытательных лабораторий орган по сертификации средств защиты информации определяет возможность, место и условия проведения испытаний, обеспечивающие объективность их результатов.

Сроки проведения испытаний устанавливаются договором между изготовителем и испытательной лабораторией.

Изготовителю должна быть предоставлена возможность ознакомиться с условиями испытаний и хранения образцов средств защиты информации в испытательной лаборатории.

При несоответствии результатов испытаний требованиям нормативных и методических документов по защите информации орган по сертификации средств защиты информации принимает решение об отказе в выдаче сертификата и направляет изготовителю мотивированное заключение. В случае несогласия с отказом в выдаче сертификата изготовитель имеет право обратиться в центральный орган системы сертификации, федеральный орган по сертификации или в Межведомственную комиссию для дополнительного рассмотрения полученных при испытаниях результатов.

10. Федеральный орган по сертификации и органы по сертификации средств защиты информации имеют право приостанавливать или аннулировать действие сертификата в следующих случаях:

>• изменение нормативных и методических документов по защите информации в части требований к средствам защиты информации, методам испытаний и контроля;

>• изменение технологии изготовления, конструкции (состава), комплектности средств защиты информации и системы контроля их качества;

>• отказ изготовителя обеспечить беспрепятственное выполнение своих полномочий лицами, осуществляющими государственные контроль и надзор, инспекционный контроль за сертификацией и сертифицированными средствами защиты информации.

11. Порядок оплаты работ по обязательной сертификации средств защиты информации определяется федеральным органом по сертификации по согласованию с Министерством финансов Российской Федерации. Оплата работ по сертификации конкретных средств защиты информации осуществляется на основании договоров между участниками сертификации.

12. Инспекционный контроль за сертифицированными средствами защиты информации осуществляют органы, проводившие сертификацию этих средств защиты информации.

13. При возникновении спорных вопросов в деятельности участников сертификации заинтересованная сторона может подать апелляцию в орган по сертификации средств защиты информации, в центральный орган системы сертификации, в федеральный орган по сертификации или в Межведомственную комиссию. Указанные организации в месячный срок рассматривают апелляцию с привлечением заинтересованных сторон и извещают подателя апелляции о принятом решении.

14. Органы, осуществляющие сертификацию средств защиты информации,

несут ответственность, установленную законодательством Российской Федерации, за выполнение возложенных на них обязанностей.

**ГОСТ Р 51275-99 ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Защита информации.**

**Объект информации. Факторы, воздействующие на информацию**

**Общие положения**

Дата введения: 2000-01-01

**1. Область применения**

Настоящий стандарт устанавливает классификацию и перечень факторов, воздействующих на защищаемую информацию, в интересах обоснования требований защиты информации на объекте информатизации.

Настоящий стандарт распространяется на требования по организации защиты информации при создании и эксплуатации объектов информатизации, используемых в различных областях деятельности (обороны, экономики, науки и других областях).

Положения настоящего стандарта подлежат применению на территории Российской Федерации органами государственной власти, местного самоуправления, предприятиями и учреждениями независимо от их организационно-правовой формы и формы собственности, должностными лицами и гражданами Российской Федерации, взявшими на себя обязательства либо обязанными по статусу исполнять требования правовых документов Российской Федерации по защите информации.

**2. Определения и сокращения**

2.1. В настоящем стандарте применяют следующие термины с соответствующими определениями:

информация — сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

защищаемая информация — информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации;

фактор, воздействующий на защищаемую информацию, — явление, действие или процесс, результатом которого могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней;

объект информатизации — совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров;

информационные ресурсы — отдельные документы и отдельные массивы документов, документы и массивы документов, содержащиеся в информационных системах (библиотеках, архивах, фондах, банках данных, информационных системах других видов);

информационная технология — приемы, способы и методы применения технических и программных средств при выполнении функций обработки информации;

обработка информации — совокупность операций сбора, накопления, ввода, вывода, приема, передачи, записи, хранения, регистрации, уничтожения, преобразования, отображения информации;

система обработки информации — совокупность технических средств и программного обеспечения, а также методов обработки информации и действий персонала, обеспечивающая выполнение автоматизированной обработки информации;

средства обеспечения объекта информатизации — технические средства и системы, их коммуникации, не предназначенные для обработки информации, но устанавливаемые вместе со средствами обработки информации на объекте информатизации;

побочное электромагнитное излучение — электромагнитное излучение, вызванное паразитной генерацией в электрических цепях технических средств обработки информации;
паразитное электромагнитное излучение — электромагнитное излучение, вызванное паразитной генерацией в электрических цепях технических средств обработки информации;
наводки — токи и напряжения в токопроводящих элементах, вызванные электромагнитными излучением, емкостными и индуктивными связями;
закладочное устройство — элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации);
программная закладка — внесенные в программное обеспечение функциональные объекты, которые при определенных условиях (входных данных) инициируют выполнение не описанных в документации функций программного обеспечения, позволяющих осуществлять несанкционированные воздействия на информацию;
программный вирус — исполняемый программный код или интерпретируемый набор инструкций, обладающий свойством несанкционированного распространения и самовоспроизведения (репликации). В процессе распространения вирусные субъекты могут себя модифицировать. Некоторые программные вирусы могут изменять, копировать или удалять программы или данные.
2.2. В настоящем стандарте приняты следующие сокращения:
ОИ — объект информатизации;
ПЭМИ — побочные электромагнитные излучения;
ТС — техническое средство.

**3. Основные положения**

3.1. Выявление и учет факторов, воздействующих или могущих воздействовать на защищаемую информацию в конкретных условиях, составляют основу для планирования и осуществления эффективных мероприятий, направленных на защиту информации на ОИ.
3.2. Полнота и достоверность выявления факторов, воздействующих на защищаемую информацию, должны быть достигнуты путем рассмотрения полного множества факторов, воздействующих на все элементы ОИ (технические и программные средства обработки информации, средства обеспечения ОИ и т. д.) и на всех этапах обработки информации.
3.3. Выявление факторов, воздействующих на защищаемую информацию, должно быть осуществлено с учетом следующих требований:
**>•** достаточности уровней классификации факторов, воздействующих на защищаемую информацию, позволяющей формировать их полное множество;
>• гибкости классификации, позволяющей расширять множества классифицируемых факторов, группировок и признаков, а также вносить изменения без нарушения структуры классификации.
3.4. Основными методами классификации факторов, воздействующих на защищаемую информацию, являются иерархический и фасетный методы.

**4. Классификация факторов, воздействующих на защищаемую информацию**

4.1. Факторы, воздействующие на защищаемую информацию и подлежащие учету при организации защиты информации, по признаку отношения к природе возникновения делят па классы:
>• субъективные;
>• объективные.
4.2. По отношению к ОИ факторы, воздействующие на защищаемую информацию, подразделяют на внутренние и внешние.
4.3. Принцип классификации факторов, воздействующих на защищаемую информацию, следующий:

>• подкласс;
>• группа;
>• подгруппа;
>• подвид.
4.3.1. Перечень объективных факторов, воздействующих на защищаемую информацию, в соответствии с установленным принципом их классификации (4.3.)
4.3.1.1. Внутренние факторы
4.3.1.1.1. Передача сигналов по проводным линиям связи
4.3.1.1.2. Передача сигналов по оптико-волоконным линиям связи
4.3.1.1.3. Излучения сигналов, функционально присущих ОИ
4.3.1.1.3.1. Излучения акустических сигналов
4.3.1.1.3.1.1. Излучения неречевых сигналов
4.3.1.1.3.1.2. Излучения речевых сигналов
4.3.1.1.3.2. Электромагнитные излучения и поля
4.3.1.1.3.2.1. Излучения в радиодиапазоне
4.3.1.1.3.2.2. Излучения в оптическом диапазоне
4.3.1.1.4. ПЭМИ
4.3.1.1.4.1. ПЭМИ сигналов (видеоимпульсов) от информационных цепей
4.3.1.1.4.2. ПЭМИ сигналов (радиоимпульсов) от всех электрических цепей ТС ОИ
4.3.1.1.4.2.1. Модуляция ПЭМИ электромагнитным сигналам от информационных цепей
4.3.1.1.4.2.2. Модуляция ПЭМИ акустическим сигналам
4.3.1.1.5. Паразитное электромагнитное излучение
4.3.1.1.5.1. Модуляция паразитного электромагнитного излучения информационными сигналами
4.3.1.1.5.2. Модуляция паразитного электромагнитного излучения акустическими сигналами
4.3.1.1.6. Наводки
4.3.1.1.6.1. Наводки в электрических цепях ТС, имеющих выход за пределы ОИ
4.3.1.1.6.1.1. Наводки в линиях связи
4.3.1.1.6.1.1.1. Наводки, вызванные побочными и (или) паразитными электромагнитными излучениями, несущими информацию
4.3.1.1.6.1.1.2. Наводки, вызванные внутренними емкостными и (или) индуктивными связями
4.3.1.1.6.1.2. Наводки в цепях электропитания
4.3.1.1.6.1.2.1. Наводки, вызванные побочными и (или) паразитными электромагнитными излучениями, несущими информацию
4.3.1.1.6.1.2.2. Наводки, вызванные внутренними емкостными и (или) индуктивными связями
4.3.1.1.6.1.2.3. Наводки через блоки питания ТС ОИ
4.3.1.1.6.1.3. Наводки в цепях заземления
4.3.1.1.6.1.3.1. Наводки, вызванные побочными и (или) паразитными электромагнитными излучениями, несущими информацию
4.3.1.1.6.1.3.2. Наводки, вызванные внутренними емкостными и (или) индуктивными связями
4.3.1.1.6.1.3.3. Наводки, обусловленные гальванической связью схемной (рабочей) «земли» узлов и блоков ТС ОИ
4.3.1.1.6.2. Наводки на ТС, провода, кабели и иные токопроводящие коммуникации и конструкции, гальванически на связанные с ТС ОИ, вызванные побочными и (или) паразитными электромагнитными излучениями, несущими информацию
4.3.1.1.7. Акустоэлектрические преобразования в элементах ТС ОИ
4.3.1.1.8. Дефекты, сбои, отказы, аварии ТС и систем ОИ
4.3.1.1.9. Дефекты, сбои и отказы программного обеспечения ОИ

4.3.1.2. Внешние факторы 4.3.1.2.1. Явления техногенного характера 4.3.1.2.1.1. Непреднамеренные электромагнитные облучения ОИ
4.3.1.2.1.2. Радиационные облучения ОИ
4.3.1.2.1.3. Сбои, отказы и аварии систем обеспечения ОИ
4.3.1.2.2. Природные явления, стихийные бедствия
4.3.1.2.2.1. Термические факторы (пожары и т. д.)
4.3.1.2.2.2. Климатические факторы (наводнения и т. д.)
4.3.1.2.2.3. Механические факторы (землетрясения и т. д.)
4.3.1.2.2.4. Электромагнитные факторы (грозовые разряды и т. д.)
4.3.1.2.2.5. Биологические факторы (микробы, грызуны и т. д.)
4.3.2. Перечень субъективных факторов, воздействующих на защищаемую информацию, в соответствии с установленным принципом их классификации (4.3.)
4.3.2.1. Внутренние факторы
4.3.2.1.1. Разглашение защищаемой информации лицами, имеющими к ней право доступа
4.3.2.1.1.1. Разглашение информации лицам, не имеющим права доступа к защищаемой информации
4.3.2.1.1.2. Передача информации по открытьм линиям связи
4.3.2.1.1.3. Обработка информации на незащищенных ТС обработки информации
4.3.2.1.1.4. Опубликование информации в открытой печати и других средствах массовой информации
4.3.2.1.1.5. Копирование информации на незарегистрированный носитель информации
4.3.2.1.1.6. Передача носителя информации лицу, не имеющему права доступа к ней
4.3.2.1.1.7. Утрата носителя с информацией 4.3.2.1.2. Неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации
4.3.2.1.2.1. Несанкционированное изменение информации
4.3.2.1.2.2. Несанкционированное копирование информации
4.3.2.1.3. Несанкционированный доступ к защищаемой информации
4.3.2.1.3.1. Подключение к техническим средствам и системам ОИ
4.3.2.1.3.2. Использование закладочных устройств
4.3.2.1.3.3. Использование программного обеспечения технических средств ОИ
4.3.2.1.3.3.1. Маскировка под зарегистрированного пользователя
4.3.2.1.3.3.2. Использование дефектов программного обеспечения ОИ
4.3.2.1.3.3.3. Использование программных закладок
4.3.2.1.3.3.4. Применение программных вирусов
4.3.2.1.3.4. Хищение носителя защищаемой информации
4.3.2.1.3.5. Нарушение функционирования ТС обработки информации
4.3.2.1.4. Неправильное организационное обеспечение защиты информации
4.3.2.1.4.1. Неправильное задание требований по защите информации
4.3.2.1.4.2. Несоблюдение требований по защите информации
4.3.2.1.4.3. Неправильная организация контроля эффективности защиты информации
4.3.2.1.5. ошибки обслуживающего персонала ОИ
4.3.2.1.5.1. Ошибки при эксплуатации ТС
4.3.2.1.5.2. Ошибки при эксплуатации программных средств
4.3.2.1.5.3. Ошибки при эксплуатации средств и систем защиты информации
4.3.2.2. Внешние факторы
4.3.2.2.1. Доступ к защищаемой информации с применением технических средств
4.3.2.2.1.1. Доступ к защищаемой информации с применением технических средств разведки
4.3.2.2.1.1.1. Доступ к защищаемой информации с применением средств

радиоэлектронной разведки
4.3.2.2.1.1.2. Доступ к защищаемой информации с применением средств оптико-электронной разведки
4.3.2.2.1.1.3. Доступ к защищаемой информации с применением средств фотографической разведки
4.3.2.2.1.1.4. Доступ к защищаемой информации с применением средств визуально-оптической разведки
4.3.2.2.1.1.5. Доступ к защищаемой информации с применением средств акустической разведки
4.3.2.2.1.1.6. Доступ к защищаемой информации с применением средств гидроакустической разведки
4.3.2.2.1.1.7. Доступ к защищаемой информации с применением средств компьютерной разведки
4.3.2.2.1.2. Доступ к защищаемой информации с использованием эффекта «высокочастотного навязывания»
4.3.2.2.1.2.1. Доступ к защищаемой информации с применением генератора высокочастотных колебаний
4.3.2.2.1.2.2. Доступ к защищаемой информации с применением генератора высокочастотного электромагнитного поля
4.3.2.2.2. Несанкционированный доступ к защищаемой информации
4.3.2.2.2.1. Подключение к техническим средствам и системам ОИ
4.3.2.2.2.2. Использование закладочных устройств
4.3.2.2.2.3. Использование программного обеспечения технических средств ОИ
4.3.2.2.2.3.1. Маскировка под зарегистрированного пользователя
4.3.2.2.2.3.2. Использование дефектов программного обеспечения ОИ
4.3.2.2.2.3.3. Использование программных закладок
4.3.2.2.2.3.4. Применение программных вирусов
4.3.2.2.2.4. Несанкционированный физический доступ на ОИ
4.3.2.2.2.5. Хищение носителя с защищаемой информацией
4.3.2.2.3. Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку
4.3.2.2.4. Действия криминальных групп и отдельных преступных субъектов
4.3.2.2.4.1. Диверсия в отношении ОИ.

**«ВРЕМЕННОЕ ПОЛОЖЕНИЕ ПО ОРГАНИЗАЦИИ РАЗРАБОТКИ, ИЗГОТОВЛЕНИЯ И ЭКСПЛУАТАЦИИ ПРОГРАММНЫХ И ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ И СРЕДСТВАХ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ» Руководящий документ Гостехкомиссии РФ**

**Принятые сокращения**

АС — автоматизированная система
ВД — временный документ
ЗАС — засекречивающая аппаратура связи
КСЗ — комплекс средств защиты
НСД — несанкционированный доступ
НТД — нормативно-техническая документация
ОС — операционная система
ППП — пакет прикладных программ
ПРД — правила разграничения доступа
РД — руководящий документ
СВТ — средства вычислительной техники
СЗИ — система защиты информации
СЗИ НСД — система защиты информации от несанкционированного доступа
СЗСИ — система защиты секретной информации СНТП — специальное научно-техническое подразделение
СРД — система разграничения доступа СУБД — система управления базами данных

ТЗ — техническое задание ЭВМ — электронно-вычислительная машина ЭВТ — электронно-вычислительная техника

**1. Общие положения**

1.1. Настоящее Положение устанавливает единый на территории Российской Федерации порядок исследований и разработок в области:

>• защиты информации, обрабатываемой автоматизированными системами различного уровня и назначения, от несанкционированного доступа;

>• создания средств вычислительной техники общего и специального назначения, защищенных от утечки, искажения или уничтожения информации за счет НСД, в том числе программных и технических средств защиты информации от НСД;

>• создания программных и технических средств защиты информации от НСД в составе систем защиты секретной информации в создаваемых АС.

1.2. Положение определяет следующие основные вопросы:

>• организационную структуру и порядок проведения работ по защите информации от НСД и взаимодействия при этом на государственном уровне;

>• систему государственных нормативных актов, стандартов, руководящих документов и требований по этой проблеме;

>• порядок разработки и приемки защищенных СВТ, в том числе программных и технических (в частности, криптографических) средств и систем защиты информации от НСД;

**>•** порядок приемки указанных средств и систем перед сдачей в эксплуатацию в составе АС, порядок их эксплуатации и контроля за работоспособностью этих средств и систем в процессе эксплуатации.

1.3. Положение разработано в развитие Инструкции № 0126-87 в части требований к программным и техническим средствам и системам защиты информации от НСД и базируется на Концепции защиты СВТ и АС от НСД к информации.

Организационные мероприятия по предупреждению утечки и защите информации, являющиеся составной частью решения проблемы защиты информации от НСД, базируются на требованиях указанной инструкции, дополняют программные и технические средства и системы и в этой части являются предметом рассмотрения настоящего Временного положения.

1.4. Временное положение обязательно для выполнения всеми органами государственного управления, государственными предприятиями, воинскими частями, другими учреждениями, организациями и предприятиями (независимо от форм собственности), обладающими государственными секретами, и предназначено для заказчиков, разработчиков и пользователей защищенных СВТ, автоматизированных систем, функционирующих с использованием информации различной степени секретности.

1.5. Разрабатываемые и эксплуатируемые программные и технические средства и системы защиты информации от НСД должны являться неотъемлемой составной частью защищенных СВТ, автоматизированных систем, обрабатывающих информацию различной степени секретности.

1.6. При разработке средств и систем защиты в АС и СВТ необходимо руководствоваться требованиями следующих руководящих документов:

>• концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации;

>• настоящее Временное положение;

>• защита от несанкционированного доступа к информации. Термины и определения;

>• средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации;

>• автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по

защите информации.

**2. Организационная структура, порядок проведения работ по защите информации от НСД и взаимодействия на государственном уровне**

2.1. Заказчиком защищенных СВТ является заказчик соответствующей АС, проектируемой на базе этих СВТ.

Заказчик защищенных СВТ финансирует их разработку или принимает долевое участие в финансировании разработок СВТ общего назначения в части реализации своих требований.

2.2. Заказчиком программных и технических средств защиты информации от НСД может являться государственное учреждение или коллективное предприятие независимо от формы собственности.

2.3. Постановку задач по комплексной защите информации, обрабатываемой автоматизированными системами, а также контроль за состоянием и развитием этого направления работ осуществляет Гостехкомиссия России.

2.4. Разработчиками защищенных СВТ общего и специального назначения, в том числе их общесистемного программного обеспечения, являются государственные предприятия — производители СВТ, а также другие организации, имеющие лицензию на проведение деятельности в области защиты информации.

2.5. Разработчиками программных и технических средств и систем защиты информации от НСД могут быть предприятия, имеющие лицензию на проведение указанной деятельности.

2.6. Проведение научно-исследовательских и опытно-конструкторских работ в области защиты секретной информации от НСД, создание защищенных СВТ общего назначения осуществляется по государственному заказу по представлению заинтересованных ведомств, согласованному с Гостехкомиссией России.

2.7. Организация и функционирование государственных и отраслевых сертификационных центров определяются Положением об этих центрах. На них возлагается проведение сертификационных испытаний программных и технических средств защиты информации от НСД. Перечень сертификационных центров утверждает Гостехкомиссия России.

**3. Система государственных нормативных актов, стандартов, руководящих документов и требований по защите информации от НСД**

3.1. Система государственных нормативных актов, стандартов, руководящих документов и требований по защите информации от НСД базируется на законах, определяющих вопросы защиты государственных секретов и информационного компьютерного права.

3.2. Система указанных документов определяет работу в двух направлениях:

>• первое — разработка СВТ общего и специального назначения, защищенных от утечки, искажения или уничтожения информации, программных и технических (в том числе криптографических) средств и систем защиты информации от НСД;

>• второе — разработка, внедрение и эксплуатация систем защиты АС различного уровня и назначения как на базе защищенных СВТ, в том числе программных и технических средств и систем защиты информации от НСД, прошедших сертификационные испытания, так и на базе средств и систем собственной разработки.

3.3. К системе документации первого направления относятся документы (в том числе, ГОСТы, РД и требования), определяющие:

>• различные уровни оснащенности СВТ средствами защиты информации от НСД и способы оценки этих уровней (критерии защищенности);

>• порядок разработки защищенных СВТ; взаимодействие, права и обязанности заказчиков и разработчиков на стадиях заказа и разработки защищенных СВТ;

>• порядок приемки и сертификации защищенных СВТ; взаимодействие, права

и обязанности заказчиков и разработчиков на стадиях приемки и сертификации защищенных СВТ;
>• разработку эксплуатационных документов и сертификатов.
3.4. К системе документации второго направления относятся документы (в том числе, ГОСТы, РД и требования), определяющие:
>• порядок организации и проведения разработки системы защиты секретной информации, взаимодействие, права и обязанности заказчика и разработчика АС в целом и СЗСИ в частности;
>• порядок разработки и заимствования программных и технических средств и систем защиты информации от НСД в процессе разработки СЗСИ;
>• порядок настройки защищенных СВТ, в том числе программных и технических средств и систем защиты информации от НСД на конкретные условия функционирования АС;
>• порядок ввода в действие и приемки программных и технических средств и систем защиты информации от НСД в составе принимаемой АС;
>• порядок использования защищенных СВТ, в том числе программных и технических средств и систем защиты информации от НСД, прошедших сертификационные испытания, в соответствии с классами и требованиями по защите в конкретных системах;
>• порядок эксплуатации указанных средств и систем;
>• разработку эксплуатационных документов и сертификатов;
>• порядок контроля защищенности АС;
>• ответственность должностных лиц и различных категорий исполнителей (пользователей) за выполнение установленного порядка разработки и эксплуатации АС в целом и СЗСИ в частности.
3.5. Состав документации, определяющей работу в этих направлениях, устанавливают Госстандарт Российской Федерации и Гостехкомиссия России.
3.6. Обязательным требованием к ТЗ на разработку СВТ и АС должно быть наличие раздела требований по защите от НСД, а в составе документации, сопровождающей выпуск СВТ и АС, должен обязательно присутствовать документ (сертификат), содержащий результаты анализа их защищенности от НСД.

**4. Порядок разработки и изготовления защищенных СВТ, в том числе программных и технических средств и систем защиты информации от НСД**

4.1. При разработке и изготовлении защищенных СВТ, в том числе программных и технических средств и систем защиты необходимо руководствоваться существующей системой разработки и постановки продукции на производство, определенной ГОСТ 21552-84 и ВД к нему, ГОСТ 16325-88 и ВД к нему, ГОСТ 15.001-88, ГОСТ 23773-88, ГОСТ 34.201-89, ГОСТ 34.602-89, РД 50-601-10-89, РД 50-601-11-89, РД 50-601-12-89 и другими документами.
4.2. Разработку защищенных СВТ общего назначения, в том числе их общесистемного программного обеспечения, осуществляют предприятия-производители СВТ по государственному заказу в соответствии с ТЗ, согласованным с Гостехкомиссией России (в случае встроенных криптографических средств и систем с Главным шифрорганом страны и предприятием-разработчиком этих средств и систем).
4.3. Разработку защищенных СВТ специального назначения, в том числе их программного обеспечения (общесистемного и прикладного), осуществляют предприятия-производители СВТ по государственному заказу в соответствии с ТЗ, согласованным с Гостехкомиссией России (в случае встроенных криптографических средств и систем — Главным шифрорганом страны и предприятием-разработчиком этих средств и систем) и утвержденным заказчиком СВТ специального назначения.
4.4. Порядок разработки защищенных программных средств на базе общесистемного программного обеспечения, находящегося в эксплуатации.
4.4.1. Разработка защищенных программных средств на базе общесистемного

программного обеспечения (ОС, СУБД, сетевые программные средства), находящегося в эксплуатации или поставляемого вместе с незащищенными СВТ предприятиями-изготовителями этих СВТ или Государственным фондом алгоритмов и программ (ГосФАП), может осуществляться по заказу для государственных нужд в соответствии с ТЗ, согласованным с разработчиком соответствующих общесистемных программных средств, с Гостехкомиссией России в пределах ее компетенции и утвержденным заказчиком этих программных средств.

4.4.2. Предприятие-разработчик общесистемного программного средства обязано в этом случае предоставить предприятию-разработчику защищенного программного средства всю необходимую документацию и оказывать консультации при разработке.

4.4.3. При необходимости, определяемой заказчиком работ, предприятие-разработчик общесистемного программного средства может быть соисполнителем разработки защищенного программного средства.

4.4.4. Разработку защищенных программных средств могут осуществлять также предприятия заинтересованных ведомств по отраслевому заказу. В этом случае ТЗ, отвечающее тем же требованиям, согласовывается головной организацией этой отрасли с Гостехкомиссией России в пределах ее компетенции и утверждается заказчиком защищенных программных средств.

4.5. Порядок разработки защищенных программных средств на базе импортных общесистемных программных прототипов.

4.5.1. Разработку (адаптацию) защищенных программных средств на базе импортных общесистемных программных прототипов осуществляют по государственному или отраслевому заказу предприятия-разработчики соответствующих типов СВТ, специализированные организации и предприятия заинтересованных ведомств по согласованию с приобретающим ведомством и в соответствии с ТЗ, согласованным с Гостехкомиссией России в пределах ее компетенции и утвержденным заказчиком этих защищенных средств в зависимости от уровня заказа.

4.5.2. Предварительным этапом разработки защищенных программных средств на базе импортных общесистемных программных прототипов является снятие защиты от копирования и вскрытия механизма работы прототипа, а также проведение анализа защитных средств прототипа на предмет их соответствия требованиям ТЗ в целях использования задействованных средств защиты, их дополнения и модификации.

Проведение работ предварительного этапа может осуществляться по отдельному ТЗ.

4.6. Порядок разработки программных средств контроля защищенности разработанных защищенных СВТ, программных средств и систем защиты.

4.6.1. Все предприятия, осуществляющие разработку защищенных СВТ, в том числе программных средств и систем защиты, обязаны разрабатывать тестовые программные средства для контроля защищенности в процессе приемки и эксплуатации защищенных СВТ и программных средств.

4.6.2. Для создания программных средств контроля могут привлекаться в качестве соисполнителей специализированные организации, имеющие на то лицензию Гостехкомиссии России, функциональной направленностью которых является «вскрытие» механизмов защиты общесистемных программных средств.

4.6.3. Создание программных средств контроля может осуществляться как по общему с разработкой защищенных средств ТЗ, так и по частному ТЗ, порядок согласования и утверждения которого аналогичен изложенному в п. 4.5.1.

4.7. Порядок разработки технических средств защиты информации от НСД.

4.7.1. Разработка технических средств защиты информации от НСД для использования в государственных структурах может производиться по государственному или отраслевому заказу.

4.7.2. Разработка технических средств защиты информации от НСД производится совместно с программными средствами, обеспечивающими их работоспособность в составе защищенных СВТ.
Кроме того, технические средства могут поддерживать защищенность общесистемных программных средств в целях безопасности информации.
4.7.3. Разработку технических средств защиты информации от НСД осуществляют как предприятия-разработчики защищенных СВТ, так и компетентные предприятия заинтересованных ведомств по ТЗ, порядок согласования и утверждения которого аналогичен изложенному в п. 4.5.1.

**5. Порядок приемки и сертификации защищенных СВТ общего и специального назначения, в том числе программных и технических средств и систем защиты информации от НСД**

5.1. Исследования (проверки, испытания) и приемка защищенных СВТ общего и специального назначения, в том числе программных и технических средств и систем защиты информации от НСД производится установленным порядком в соответствии с ГОСТ В15.307-77, ГОСТ В15.210-78, ГОСТ 23773-88 и НТД по безопасности информации.
5.2. Сертификационные испытания защищенных СВТ общего и специального назначения, в том числе программных и технических средств и систем защиты информации от НСД проводят государственные и отраслевые сертификационные центры.
5.3. Право на проведение сертификационных испытаний защищенных СВТ, в том числе программных и технических средств и систем защиты информации от НСД предоставляется Гостехкомиссией России по согласованию с Госстандартом России и в случае использования криптографических средств и систем защиты с Главным шифрорганом страны, предприятиям-разработчикам защищенных СВТ, специализированным организациям ведомств, разрабатывающих защищенные СВТ, в том числе программные и технические средства и системы защиты информации от НСД.
5.4. В соответствии с Положением о сертификации средств и систем вычислительной техники и связи по требованиям защиты информации по результатам сертификационных испытаний оформляется акт, а разработчику выдается сертификат, заверенный Гостехкомиссией России и дающий право на использование и распространение этих средств как защищенных.
5.5. Средства, получившие сертификат, включаются в номенклатуру защищенных СВТ, в том числе программных и технических средств и систем защиты информации от НСД.
Обработка секретной информации разрешается только с использованием сертифицированных средств и систем защиты.
5.6. Разработанные программные средства после их приемки представляются для регистрации в специализированный фонд Государственного фонда алгоритмов и программ.

**6. Порядок разработки, сертификации, внедрения и эксплуатации средств криптографической защиты информации от несанкционированного доступа**

6.1. Данный раздел определяет взаимодействие сторон и порядок проведения работ при создании, сертификации и эксплуатации средств криптографической защиты информации (СКЗИ) от несанкционированного доступа на государственных предприятиях, в ведомствах.
Действие данного раздела распространяется на программные, технические и программно-технические средства в составе СВТ и АС, применяемые для криптографической защиты от НСД к информации, обрабатываемой, хранимой, накапливаемой и передаваемой в вычислительных системах, построенных на базе отдельных ЭВМ, комплексов ЭВМ и локальных вычислительных сетей, расположенных в пределах одной контролируемой зоны.
Разрешается применение положений данного раздела также в случае нескольких контролируемых зон при условии, что для связи между ними используются защищенные с помощью аппаратуры ЗАС или СКЗИ каналы, по

которым в соответствии с действующими нормативными документами разрешена передача секретной информации соответствующего грифа (см. п. 6.15 данного раздела).
В дальнейшем: Положение о сертификации.
6.2. Организационно-методическое руководство работами по созданию и эксплуатации СКЗИ, сертификацию СКЗИ, а также контроль за состоянием и развитием этого направления работ осуществляют Гостехкомиссия России и Главный шифрорган страны при посредстве ряда уполномоченных ими специализированных организаций.
6.3. С помощью СКЗИ может осуществляться защита от несанкционированного доступа к несекретной и служебной информации, а также к информации, имеющей грифы «Секретно», «Совершенно секретно» и «Особой важности».
6.4. При выполнении разработки СКЗИ (или изделия СВТ, содержащего в своем составе СКЗИ), предназначаемого для защиты секретной информации любых грифов, а также для защиты ценной и особо ценной информации, техническое задание на СКЗИ должно быть согласовано с Гостехкомиссией России и Главным шифрорганом страны.
Вместе с техническим заданием должны быть направлены схема конфигурации защищаемых СВТ или АС, описание структуры подлежащих защите информационных объектов (с указанием максимального грифа секретности), а также данные о характеристиках допуска и предполагаемых административных структурах пользователей.
6.5. По результатам рассмотрения исходных данных вышеупомянутые органы представляют разработчику СКЗИ рекомендации по использованию одного из аттестованных алгоритмов шифрования, а также (при необходимости) описание его криптосхемы, криптографические константы, тестовые примеры для проверки правильности реализации алгоритма, рекомендации по построению ключевой системы СКЗИ и ряд других документов.
6.6. На основе полученных документов разработчик реализует СКЗИ в виде программного или технического изделия и с привлечением специализированных организаций готовит необходимые материалы для сертификации СКЗИ в соответствии с Положением о сертификации.
Приемку полученных в результате разработки опытных образцов осуществляет комиссия, создаваемая Заказчиком СКЗИ. В состав комиссии должны быть включены представители Гостехкомиссии России и Главного шифроргана страны.
6.7. Сертификация СКЗИ осуществляется на хозрасчетных началах. Положительная сертификация СКЗИ завершается выдачей сертификационного удостоверения.
6.8. Применение СКЗИ, не прошедших в установленном порядке сертификацию для защиты от НСД к секретной информации любых грифов, а также ценной и особо ценной информации запрещается.
6.9. При внедрении АС, содержащей в своем составе сертифицированное СКЗИ и при условии, что данная АС предназначается для обработки секретной информации с грифом не выше «Совершенно секретно» или для обработки ценной информации, дополнительного разрешения на эксплуатацию сертифицированного СКЗИ не требуется (кроме случаев, специально оговоренных в сертификационном удостоверении на СКЗИ).
Для АС, предназначенных для обработки информации с грифом «Особой важности» или для обработки особо ценной информации, должно быть получено письменное разрешение Гостехкомиссии России и Главного шифроргана страны на эксплуатацию СКЗИ в составе конкретной АС.
6.10. Эксплуатация СКЗИ, применяемых для защиты секретной или ценной информации, должна осуществляться в соответствии с требованиями разрабатываемых Инструкции по обеспечению безопасности эксплуатации СКЗИ в составе АС и Инструкции о порядке использования действующих сменных ключей.

В организации, осуществляющей эксплуатацию АС, должна быть создана служба (орган) безопасности информации, на которую возлагаются ответственность за реализацию мероприятий, предусмотренных вышеназванными инструкциями.

6.11. Гриф секретности действующих сменных ключей и соответствующих ключевых документов при защите информации от НСД с помощью СКЗИ, должен соответствовать максимальному грифу секретности информации, шифруемой с использованием этих ключей.

Носители с записанной на них ключевой документацией СКЗИ учитываются, хранятся и уничтожаются как обычные документы соответствующего грифа секретности согласно Инструкции по обеспечению режима секретности № 0126-87.

6.12. СКЗИ без введенных криптографических констант и действующих сменных ключей имеют гриф секретности, соответствующий грифу описания криптосхемы. СКЗИ с загруженными криптографическими константами имеет гриф секретности, соответствующий грифу криптографических констант. Гриф секретности СКЗИ с загруженными криптографическими константами и введенными ключами определяется максимальным грифом содержащихся в СКЗИ ключей и криптографических констант.

6.13. Шифртекст, полученный путем зашифрования с помощью СКЗИ открытой секретной информации любых грифов, является несекретным.

Внешние носители данных (магнитные ленты, диски, кассеты, дискеты и т. п.) с зашифрованной информацией могут пересылаться, храниться и учитываться как несекретные, если они не содержат и ранее не содержали открытой секретной информации.

6.14. Для передачи за пределы контролируемой зоны шифртекста, полученного путем зашифрования с помощью СКЗИ несекретной информации, могут использоваться незащищенные каналы связи.

Если гриф исходной информации (до зашифрования) был «Для служебного пользования», то допускается применение только сертифицированного СКЗИ.

6.15. Для передачи за пределы контролируемой зоны шифртекста, полученного путем зашифрования с помощью СКЗИ информации с грифами «Секретно» и выше, должны использоваться каналы связи, защищенные с помощью связной шифраппаратуры, для которых в соответствии с действующими нормативными документами получено разрешение на передачу секретной информации. Специальное разрешение на эксплуатацию СКЗИ в этом случае не требуется.

Порядок создания шифраппаратуры, т. е. криптографических средств различных видов (технических и программно-технических), предназначенных для защиты информации, передаваемой за пределы контролируемой зоны по незащищенным каналам связи, регламентируется Положением о разработке, изготовлении и обеспечении эксплуатации шифровальной техники, государственных и ведомственных систем связи и управления и комплексов вооружения, использующих шифровальную технику (Положение ПШ-89), утвержденным Постановлением Совета Министров СССР от 30.04.90 г. № 439-67.

6.16. Ответственность за надлежащее исполнение правил эксплуатации СКЗИ (в том числе в период проведения приемочных испытаний), возлагается на руководство предприятий, эксплуатирующих данные СКЗИ.

6.17. Контроль за выполнением требований инструкций по эксплуатации СКЗИ возлагается на службы защиты информации предприятий, эксплуатирующих данные СКЗИ.

**7. Порядок организации и проведения разработок системы защиты секретной информации в ведомствах и на отдельных предприятиях**

7.1. Для решения научно-технических, методических и принципиальных практических вопросов по проблеме защиты информации от НСД в АС в системе ведомств может проводиться комплекс научно-исследовательских и

опытно-конструкторских работ по отраслевым планам.
7.2. В целях организации проблемных исследований, централизации разработок средств и систем защиты информации от НСД, осуществления научно-методического руководства проведением работ по этой проблеме в системе ведомств при головных организациях по АС могут создаваться специализированные отраслевые подразделения, осуществляющие взаимодействие с аналогичными подразделениями других министерств и ведомств.
7.3. Научное руководство работами по защите информации от НСД осуществляет главный конструктор интегрированных АС страны.
7.4. Общее руководство работами по защите информации от НСД, осуществление единой технической политики, организационно-методическое руководство и координацию работ, финансирование НИОКР по отраслевым заказам, взаимодействие с Гостехкомиссией России, другими ведомствами, а также контроль за организацией и проведением работ по защите информации от НСД в центральных аппаратах ведомств осуществляют научно-технические и режимные подразделения или назначаются кураторы этого направления работ.
7.5. На предприятии научно-техническое руководство и непосредственную организацию работ по созданию СЗСИ интегрированной АС осуществляет главный конструктор этой системы, а по типам АС — главные конструкторы этих систем, научные руководители тем, начальники объектов ЭВТ или другие должностные лица, обеспечивающие научно-техническое руководство всей разработкой соответствующей АС.
7.6. При разработке системы защиты в АС следует руководствоваться классификацией автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требованиями по защите информации в автоматизированных системах различных классов.
Система защиты секретной информации реализуется в виде подсистемы АС и включает комплекс организационных, программных, технических (в том числе криптографических) средств, систем и мероприятий по защите информации от НСД. СЗСИ состоит из системной и функциональной частей. Системная часть является общей и применяется при разработке, внедрении и эксплуатации всех или большинства задач АС, функциональная часть обеспечивает защиту информации при решении конкретных задач.
7.7. Разработку СЗСИ АС осуществляют подразделение, разрабатывающее на предприятии АС, группа или отдельные специалисты по разработке средств и мер защиты и (или) специализированные научно-исследовательские, конструкторские и проектные предприятия (в том числе других министерств и ведомств) по договорам, заключаемым заказчиком АС.
В структуре крупных подразделений с большим объемом работ по режимному обеспечению выделяются также службы безопасности или секретные органы.
7.8. На подразделение разработки средств и мер защиты информации возлагаются разработка и внедрение системного режимного обеспечения (адаптация и настройка программных и технических средств и систем централизованной разработки), а также разработка требований к функциональному режимному обеспечению.
К разработке и внедрению системного режимного обеспечения привлекаются специалисты — разработчики обеспечивающих и функциональных подсистем АС, служб безопасности или секретных органов.
Разработка и внедрение режимного обеспечения АС осуществляется при взаимодействии со специальными научно-техническими подразделениями — службами защиты информации и подразделениями режимно-секретной службы предприятия.
7.9. Методическое руководство и участие в разработке требований по защите информации от НСД, аналитического обоснования необходимости создания режимного обеспечения АС, согласование выбора СВТ (в том числе

общесистемного программного обеспечения), программных и технических средств и систем защиты, организацию работ по выявлению возможностей и предупреждению утечки секретной информации при ее автоматизированной обработке осуществляет СНТП предприятия.
В выработке требований по защите информации от НСД СНТП участвует совместно с заказчиком соответствующей АС, отраслевым органом обеспечения безопасности и военным представительством Министерства обороны в части вопросов, относящихся к его компетенции.
7.10. Общее руководство работами по обеспечению режима секретности при разработке АС осуществляет заместитель руководителя предприятия-разработчика по режиму.
Общее руководство работами по обеспечению режима секретности при эксплуатации АС осуществляет заместитель руководителя предприятия (организации), отвечающий за обеспечение режима секретности.
Организацию контроля эффективности средств и мер защиты информации разрабатывает предприятие и осуществляет руководитель, отвечающий на предприятии за организацию работ по защите информации.
7.11. При разработке СЗСИ необходимо максимально использовать имеющиеся или разрабатываемые типовые общесистемные компоненты, заимствуя программные и технические средства и системы защиты информации от НСД централизованной разработки, используя защищенные СВТ.
7.12. В рамках существующих стадий и этапов создания АС (ГОСТ 34.601-90) выполняются необходимые этапы работ по созданию СЗСИ.
7.13. В комплексе работ по созданию АС должны предусматриваться опережающая разработка и внедрение системной части СЗСИ.
7.14. На предпроектной стадии по обследованию объекта автоматизации группой обследования, назначенной приказом заказчика АС:
>• устанавливается наличие или отсутствие секретной информации в АС, подлежащей разработке, оценивается ее степень секретности и объемы;
>• определяются режим обработки секретной информации, класс АС, комплекс основных технических СВТ, общесистемные программные средства, предполагаемые к использованию в разрабатываемой АС;
>• оценивается возможность использования типовых или разрабатываемых централизованно и выпускаемых серийно средств защиты информации;
>• определяются степень участия персонала ВЦ, функциональных и производственных служб, научных и вспомогательных работников объекта автоматизации в обработке информации, характер взаимодействия между собой и с подразделениями режимно-секретной службы;
>• определяются мероприятия по обеспечению режима секретности на стадии разработки секретных задач.
7.15. На основании результатов предпроектного обследования разрабатываются аналитическое обоснование создания СЗСИ и раздел ТЗ на ее отработку.
7.16. На стадии разработки проектов СЗСИ заказчик контролирует ее разработку.
7.17. На стадиях технического и рабочего проектирования разработчик системной части СЗСИ обязан:
>• уточнить состав средств защиты в применяемых версиях ОС и ППП, описать порядок их настройки и эксплуатации, сформулировать требования к разработке функциональных задач и баз данных АС;
>• разработать или адаптировать программные и технические средства защиты, разработать организационные мероприятия по системной части СЗСИ;
>• разработать организационно-распорядительную и проектную документацию СЗСИ и рабочую документацию по эксплуатации средств и мер защиты;
>• осуществлять методическую помощь разработчикам функциональной части СЗСИ.

7.18. На стадиях технического и рабочего проектирования разработчик функциональной части СЗСИ обязан:
>• представить разработчику системной части СЗСИ необходимые исходные данные для проектирования;
>• при методической помощи разработчиков системной части СЗСИ предусмотреть при решении функциональных задач АС использование средств и мер защиты;
>• разработать проектную документацию по режимному обеспечению задачи АС и рабочие инструкции для эксплуатации функциональных задач АС, определяющие порядок работы персонала ВЦ и пользователей при обработке секретной информации с учетом функционирования СЗСИ;
>• обосновать количество лиц (и их квалификацию), необходимых для непосредственной эксплуатации (применения) разработанных средств (системы) защиты секретной информации;
>• определить порядок и условия использования стандартных штатных средств защиты обрабатываемой информации, включенных разработчиком в ОС, ППП и т.п.;
>• выполнить генерацию пакета прикладных программ в комплексе с выбранными стандартными средствами защиты.
7.19. Разработка, внедрение и эксплуатация СЗСИ АС осуществляется в отрасли или на отдельном предприятии в соответствии с требованиями следующей организационно-распорядительной и проектной документацией, учитывающей конкретные условия функционирования АС различного уровня и назначения:
>• Положение о порядке организации и проведения в отрасли (на предприятии) работ по защите секретной информации в АС;
>• Инструкция по защите секретной информации, обрабатываемой в АС отрасли (на предприятии или в подразделениях предприятия);
>• раздел Положения о разрешительной системе допуска исполнителей к документам и сведениям на предприятии, определяющий особенности системы допуска в процессе разработки и функционирования АС;
приказы, указания, решения:
>• о создании соответствующих подразделений разработчиков, о формировании группы обследования, о создании экспертных комиссий;
>• о начале обработки на объекте ЭВТ информации определенной степени секретности;
>• о назначении лиц, ответственных за эксплуатацию вычислительной системы, баз данных СЗСИ;
>• о назначении уполномоченных службы безопасности и т.д.;
>• проектная документация различных стадий создания СЗСИ.
7.20. Разработка, внедрение и эксплуатация СЗСИ в АС производится установленным порядком в соответствии с требованиями ГОСТ 34.201-89, ГОСТ 34.602-89, ГОСТ 34.601-90, РД 50-680—88, РД 50-682-89, РД 50-34.698-90 и других документов.
21. Модернизация АС должна рассматриваться как самостоятельная разработка самой АС и СЗСИ для нее. Организация работ при этом должна соответствовать содержанию настоящего раздела.

**8. Порядок приемки СЗСИ перед сдачей в эксплуатацию в составе АС**

8.1. На стадии ввода в действие КСЗ осуществляются:
>• предварительные испытания средств защиты;
>• опытная эксплуатация средств защиты и функциональных задач АС в условиях их работы;
>• приемочные испытания средств защиты;
>• приемочные испытания СЗСИ в составе автоматизированной системы комиссией соответствующего ранга.
8.2. Предварительные испытания средств защиты проводит разработчик этих средств совместно с заказчиком и с привлечением специалистов отраслевых

органов безопасности информации в целях проверки отдельных средств по ГОСТ 21552-84, ГОСТ 16325-88 и ГОСТ 23773-88, соответствия технической документации требованиям ТЗ, выработки рекомендаций по их доработке и определения порядка и сроков проведения опытной эксплуатации.

8.3. Допускается проведение опытной эксплуатации средств защиты до эксплуатации функциональных задач АС или параллельно с ней. Опытную эксплуатацию осуществляет заказчик с участием разработчика в соответствии с программой в целях проверки работоспособности средств защиты на реальных данных и отработки технологического процесса. На этапе опытной эксплуатации допускается обработка информации, имеющей гриф «Секретно» и «Совершенно секретно».

Для информации, имеющей гриф «Особой важности», возможность обработки на этапе опытной эксплуатации определяют совместно заказчик, разработчик и отраслевой орган безопасности информации.

Опытная эксплуатация функциональных задач АС должна включать проверку их функционирования в условиях работы средств защиты.

8.4. При положительных результатах опытной эксплуатации все программные, технические средства, организационная документация сдаются заказчику по акту.

Приемка технических средств защиты в эксплуатацию заключается в проверке их характеристик и функционирования в конкретных условиях, а программных средств защиты — в решении контрольного примера (теста), наиболее приближенного к конкретным условиям функционирования АС, с запланированными попытками обхода систем защиты. Контрольный пример готовят разработчики совместно с заказчиком.

8.5. Приемочные испытания СЗСИ проводятся в составе автоматизированной системы, предъявляемой комиссии заказчика.

Ответственность за организацию работ при вводе в действие СЗСИ, за функционирование средств защиты после приемочных испытаний несет заказчик.

8.6. Отчетные материалы по результатам приемочных испытаний СЗСИ оформляются в соответствии с ГОСТ 34.201-89 и РД 50-34.698-90 и направляются в орган по сертификации для оформления сертификата.

Виды документов на программные средства защиты определены ГОСТ 19.101-77, на технические средства — ГОСТ 2.102-68, а на эксплуатационные документы — ГОСТ 2.601-68.

**9. Порядок эксплуатации программных и технических средств и систем защиты секретной информации от НСД**

9.1. Обработка информации в АС должна производиться в соответствии с технологическим процессом обработки секретной информации, разработанным и утвержденным в порядке, установленном на предприятии для проектирования и эксплуатации АС.

9.2. Для эксплуатации СЗСИ — комплекса программно-технических средств и организационных мероприятий по их сопровождению, направленного на исключение несанкционированного доступа к обрабатываемой в АС информации, приказом руководителя предприятия (структурного подразделения) назначаются лица, осуществляющие:

**>•** сопровождение СЗСИ, включая вопросы организации работы и контроля за использованием СЗСИ в АС;

**>•** оперативный контроль за функционированием СЗСИ;

>• контроль соответствия общесистемной программной среды эталону;

**>•** разработку инструкции, регламентирующей права и обязанности операторов (пользователей) при работе с секретной информацией.

**10. Порядок контроля эффективности защиты секретной информации в АС**

10.1. Контроль эффективности защиты информации в АС проводится в целях проверки сертификатов на средства защиты и соответствия СЗИ требованиям стандартов и нормативных документов Гостехкомиссии России по защите

информации от НСД на следующих уровнях:
>• государственном, осуществляемом Инспекцией Гостехкомиссии России по оборонным работам и работам, в которых используются сведения, составляющие государственную тайну;
>• отраслевом, осуществляемом ведомственными органами контроля (главными научно-техническими и режимными управлениями, головными организациями по защите информации в АС);
>• на уровне предприятия (отдельной организации), осуществляемом военными представительствами Вооруженных Сил (по оборонным работам), специальными научно-техническими подразделениями и режимно-секретными службами (органами, службами безопасности).
10.2. Инициатива проведения проверок принадлежит организациям, чья информация обрабатывается в АС, Гостехкомиссии России и ведомственным (отраслевым) органам контроля.
10.3. Проверка функционирующих средств и систем защиты информации от НСД осуществляется с помощью программных (программно-технических) средств на предмет соответствия требованиям ТЗ с учетом классификации АС и степени секретности обрабатываемой информации.
10.4. По результатам проверки оформляется акт, который доводится до сведения руководителя предприятия, пользователя и других организаций и должностных лиц в соответствии с уровнем контроля.
10.5. В зависимости от характера нарушений, связанных с функционированием средств и систем защиты информации от НСД, действующей АС в соответствии с положением о Гостехкомиссии России могут быть предъявлены претензии вплоть до приостановки обработки информации, выявления и устранения причин нарушений.
Возобновление работ производится после принятия мер по устранению нарушений и проверки эффективности защиты органами контроля и только с разрешения органа, санкционировавшего проверку.
В случае прекращения работ по результатам проверки Инспекцией Гостехкомиссии России они могут быть возобновлены только с разрешения Гостехкомиссии России, а в отношении должностных лиц, виновных в этих нарушениях, решается вопрос о привлечении их к ответственности в соответствии с требованиями Инструкции № 0126-87 и действующим законодательством.

**11. Порядок обучения, переподготовки и повышения квалификации специалистов в области защиты информации от НСД**

11.1. Подготовка молодых специалистов и переподготовка кадров в области защиты информации, обрабатываемой в АС, от НСД осуществляется в системе Госкомитета Российской Федерации по делам науки и высшей школы и Вооруженных Сил кафедрами вычислительной техники и автоматизированных систем высших учебных заведений по договорам с министерствами, ведомствами и отдельными предприятиями.
11.2. Подготовка осуществляется по учебным программам, согласованным с Гостехкомиссией России.
11.3. Повышение квалификации специалистов, работающих в этой области, осуществляют межотраслевые и отраслевыми институты повышения квалификации и вышеуказанные кафедры вузов по программам, согласованным с Гостехкомиссией России и отраслевыми органами контроля.

**«ПОЛОЖЕНИЕ**
**О ГОСУДАРСТВЕННОМ ЛИЦЕНЗИРОВАНИИ ДЕЯТЕЛЬНОСТИ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ» Совместное решение Гостехкомиссии России и ФАПСИ № 10 от 27 апреля 1994 г.**

1.1. Настоящее Положение устанавливает основные принципы, организационную структуру системы государственного лицензирования деятельности предприятий, организаций и учреждений (далее — предприятий) независимо от их ведомственной принадлежности и форм

собственности в области защиты информации, обрабатываемой (передаваемой) техническими средствами, а также порядок лицензирования и контроля за деятельностью предприятий, получивших лицензии.

1.2. Система Государственного лицензирования предприятий в области защиты информации является составной частью Государственной системы защиты информации.

Деятельность системы Государственного лицензирования организуют Государственная техническая комиссия при Президенте Российской Федерации (Гостехкомиссия России), Федеральное агентство правительственной связи и информации при Президенте Российской Федерации (ФАПСИ) и другие министерства и ведомства в пределах компетенции, установленной законодательством Российской Федераций.

1.3. Государственному лицензированию подлежат следующие виды деятельности по защите информации.

1.3.1. Гостехкомиссией России:

а) сертификация защищенных средств обработки информации, средств защиты и контроля защищенности информации, программных средств по требованиям безопасности информации;

б) аттестование объектов информатики(СМ.Сноску 1) на соответствие требованиям по безопасности информации;

в) специсследования на побочные электромагнитные излучения и наводки технических средств обработки информации (ТСОИ) на соответствие требованиям по безопасности информации;

г) экспертиза программных средств защиты информации и защищенных программных средств обработки информации на соответствие требованиям по предотвращению несанкционированного доступа к информации;

д) создание, монтаж, наладка, установка, ремонт, сервисное обслуживание технических средств защиты информации, защищенных ТСОИ, технических средств контроля эффективности мер защиты информации, программных средств защиты информации, защищенных программных Средств обработки информации, программных средств контроля защищенности информации;

е) проектирование объектов информатики в защищенном исполнении;

ж) контроль защищенности, информации в ТСОИ и на объектах информатики.

1.3.2. ФАПСИ:

а) разработка, производство, проведение сертификационных испытаний, реализация, эксплуатация шифровальных средств, предназначенных для криптографической защиты информации, содержащей сведения, составляющие государственную или иную охраняемую законом тайну, при ее обработке, хранении и передаче по каналам связи, а также предоставление услуг в области шифрования этой информации;

б) разработка, производство, проведение сертификационных испытаний, эксплуатация систем и комплексов телекоммуникаций высших органов государственной власти Российской Федерации;

1.4. Государственная лицензия на право деятельности по защите информации выдается подавшему заявку на получение такой лицензии предприятию, располагающему необходимой испытательной базой, нормативной и

___

Сноска 1. Под объектами информатики понимаются автоматизированные системы, системы связи, отображения и размножения вместе с помещениями, в которых они установлены, предназначенные для обработки и передачи информации, подлежащей защите, а также помещения, предназначенные для ведения конфиденциальных переговоров.

___

методической документацией, научным и инженерно-техническим персоналом, обладающим современным уровнем знаний в соответствующей области деятельности на основании результатов экспертизы деятельности

предприятия по заявленному направлению работ.
1.5. Лицензии на реализацию и эксплуатацию шифровальных средств, закрытых систем и комплексов телекоммуникаций, а также на предоставление услуг в области шифрования информации выдаются предприятиям только при наличии сертификатов ФАПСИ на указанные средства, системы и комплексы.
1.6. Лицензиат, предоставляющий услуги по шифрованию информации, обязан обеспечить тайну переписки, телефонных переговоров, документальных и иных сообщений лиц, пользующихся этими услугами, а в необходимых случаях обеспечить возможность проведения оперативно-розыскных и следственных мероприятий в соответствии с действующим законодательством Российской Федерации.
1.7. Лицензии на использование шифровальных средств, закрытых систем и комплексов телекоммуникаций для криптографической защиты информации при передаче ее по каналам взаимоувязанной сети связи (ВСС) выдаются только при наличии соответствующих сертификатов и лицензий Министерства связи Российской Федерации.
1.9. Государственная лицензия выдается заявителю на конкретный вид деятельности на срок до 3-х лет, по истечению которых лицензия продлевается на очередные три года, установленным в п. 3.1.4. порядком.
1.10. Лицензиаты несут юридическую и финансовую ответственность за полноту и качество выполнения работ и обеспечение сохранности государственных и коммерческих секретов, доверенных им в ходе практической деятельности.
1.11. Юридические и физические лица, осуществляющие деятельность, виды которой указаны в п. 1.3. настоящего Положения, без лицензии или нарушившие установленные правила лицензирования деятельности несут ответственность, предусмотренную законодательством Российской Федерации.
2.1. Организационную структуру государственной системы лицензирования деятельности предприятий в области защиты информации образуют:
>• государственные органы по лицензированию;
**>•** отраслевые (ведомственные, региональные) лицензионные центры (далее — лицензионные центры);
>• предприятия-заявители (лицензируемые предприятия, лицензиаты);
**>•** предприятия и организации, в том числе заказывающие управления (заказчики), размещающие работы по защите информации (далее — предприятия-потребители).
2.2. Государственными органами по лицензированию являются Гостехкомиссия России, ФАПСИ, которые в пределах своей компетенции осуществляют следующие функции:
>• организуют обязательное государственное лицензирование деятельности предприятий;
**>•** выдают государственные лицензии предприятиям-заявителям по представлению лицензионных центров;
**>•** осуществляют научно-методическое руководство лицензионной деятельностью;
>• осуществляют контроль и надзор за соблюдением правил лицензирования, полнотой и качеством проводимых лицензиатами работ на объектах информатики;
>• обеспечивают публикацию необходимых сведений о ходе и порядке лицензирования;
>• рассматривают спорные вопросы, возникающие в ходе лицензирования.
2.3. Лицензионные центры осуществляют следующие функции:
>• формируют экспертные комиссии и представляют их состав на утверждение в соответствующие государственные органы по лицензированию;
>• планируют и проводят работы по экспертизе заявителей;

>• готовят по результатам экспертизы представления в соответствующие государственные органы по лицензированию;
>• контролируют полноту и качество выполненных лицензиатами работ;
>• систематизируют отчеты лицензиатов и представляют сводный отчет в соответствующие государственные органы по лицензированию ежегодно;
>• принимают участие в работе соответствующих государственных органов по лицензированию при рассмотрении спорных вопросов, возникающих в процессе лицензирования, и фактов некачественной работы лицензиатов.
Лицензионные центры назначаются совместными приказами руководства соответствующих государственных органов по лицензированию и отраслей промышленности, ведомств, органов регионального управления.
2.3.1. Для всестороннего обследования предприятий-заявителей с целью оценки их возможностей проводить работы в избранном направлении защиты информации и вынесения по материалам обследования заключения о возможности предоставления им права на эти работы при лицензионных центрах создаются экспертные комиссии.
Экспертные комиссии формируются из числа компетентных в соответствующей области защиты информации специалистов отраслей промышленности, Вооруженных Сил, органов государственного управления, других организаций и учреждений.
2.4. Лицензиаты имеют право пользоваться нормативно-методическими документами соответствующих государственных органов по лицензированию, обращаться к ним за необходимыми консультациями и содействием, а также ссылаться в официальных документах и рекламных материалах на полученную лицензию.
2.5. Предприятия-потребители имеют право обращаться с рекламациями на некачественно выполненные лицензиатами работы по защите информации в соответствующий лицензионный центр либо непосредственно в государственный орган по лицензированию.
3.2. Контроль и надзор за полнотой и качеством проводимых лицензиатами работ на объектах информатики осуществляется:
>• в ходе проверок Гостехкомиссией России, ФАПСИ и отраслевыми органами контроля состояния защиты на предприятиях-потребителях, воспользовавшихся услугами лицензиатов;
>• при контроле Гостехкомиссией России, ФАПСИ, лицензионными центрами качества выполненных лицензиатами работ по рекламациям предприятий-потребителей.
В зависимости от характера выявленных нарушений к лицензиатам могут быть применены следующие санкции:
>• поручение устранить за свой счет выявленные недостатки;
>• лишение лицензии.
Возмещение понесенных предприятием-потребителем затрат (ущерба) в случаях выявления нарушений состояния защиты производится в судебном порядке через хозяйственный суд (арбитраж).

**Основные требования к предприятиям-заявителям на право получения лицензий в области защиты информации**

К предприятиям-заявителям на право получения лицензий предъявляются требования по:
>• уровню квалификации специалистов;
>• наличию и качеству измерительной базы;
>• наличию и качеству производственных помещений;
>• наличию режимного органа и обеспечению охраны материальных ценностей и секретов заказчика.
1.1. Специалисты предприятий-заявителей на право получения лицензий должны ЗНАТЬ (в пределах своих функциональных обязанностей):
>• основные руководящие документы по обеспечению защиты информации и контролю ее эффективности;

>• нормативно-методические документы по защите и контролю защищенности информации, циркулирующей в технических средствах ее передачи и обработки и в помещениях, предназначенных для ведения служебных (секретных) переговоров;
>• необходимое программно-аппаратное оснащение подразделений защиты информации и контроля ее защищенности;
>• устройство, технические характеристики, принципы работы технических средств (по направлениям деятельности). Принципы формирования информативных сигналов в системах (технических средствах) обработки, передачи информации и пути циркуляции этих сигналов. Схемно-конструктивные решения основных типов технических средств информатики;
>• физические основы возникновения каналов утечки информации при ее обработке в средствах информатики и ведении служебных переговоров в выделенных помещениях. Временные, частотные, амплитудные и спектральные характеристики аналоговых и дискретных сигналов, циркулирующих в средствах информатики, и выделенных помещениях. Отличительные особенности информативных сигналов каждого вида технических средств передачи и обработки информации. Теоретические основы распространения электромагнитных полей в ближней и дальней зонах;
>• возможные каналы утечки секретной информации при ее обработке, передаче, хранении и отображении в средствах информатики и акустической информации, циркулирующей в выделенных помещениях. Причины возникновения паразитной генерации, электроакустических преобразований, побочных электромагнитных излучений, неравномерности потребления тока в сети электропитания и наводок на токопроводящие цепи, вспомогательные коммуникации и другие металлоконструкции при работе технических средств информатики;
>• структуру и функции программных средств управления вычислительным процессом (операционные системы, сетевые пакеты, системы управления базами данных). Принципы системного и прикладного алгоритмирования и программирования. Языки программирования. Принципы организации мультиплексных, многопользовательских и монопольных режимов работы средств информатики;
>• возможности технических средств разведки по добыванию информации или нарушению ее целостности;
>• основные программные, технические, организационные и режимные меры защиты информации от разрушения, искажения, копирования и утечки за счет несанкционированных действий как пользователей, так и лиц, недопущенных к обрабатываемой информации. Методы обеспечения разграничения и контроля доступа. Рекомендованные аппаратные и программные средства шифрования и криптографии, защиты от программ «вирусов» и закрытия физических каналов утечки информации, порядок и способы их применения;
>• возможности и технические характеристики программных и аппаратных средств защиты информационных технологий и информации, циркулирующей в выделенных помещениях, и комплексного контроля эффективности систем защиты информации;
>• требования к тест-программам, применяемым при измерении уровня побочных электромагнитных излучений средств информатики. Основные тест-программы, принципы их работы, возможность использования (применимость) для проверки конкретных типов технических, средств информатики и выделенных помещений;
5^ требования к тест-программам по проверке систем защиты от несанкционированного доступа. Основные тест- программы, принципы их работы, возможность использования (применимость) для проверки на конкретных типах технических средств вычислительной техники и порядок их использования при проверке;

>• метрологические требования к техническим средствам и условиям проведения измерений;
>• организацию работ и предприятия, обеспечивающие техническое обслуживание, ремонт и метрологическую поверку аппаратуры контроля;
>• принципы работы применяемой контрольно-измерительной аппаратуры, ее тактико-технические характеристики и возможности.
1.2. Специалисты предприятий-заявителей на право получения лицензий должны УМЕТЬ:
>• планировать и организовывать мероприятия по проведению специсследований технических средств информатики, аттестации и комплексного технического контроля эффективности систем защиты информации, циркулирующей в средствах информатики и выделенных помещениях на проверяемых объектах. Анализировать полученные результаты;
>• готовить отчетные документы по результатам проведенной работы;
>• определять характеристики и параметры контролируемого средства или выделенного помещения и проводить их анализ;
>• определять состав и структуру системы защиты информации, ее организационное и программно-аппаратное обеспечение. Проверять полноту соответствия технической документации требованиям нормативно-методических документов. Выявлять возможные каналы утечки или несанкционированного доступа к информации;
>• применять средства криптографической защиты;
>• организовать работу и применять средства защиты от специального программного воздействия (программ-"вирусов");
>• выявлять нарушения в технологии обработки информации. С применением программных, аппаратных и аналитических методов проверять правильность функционирования систем разграничения доступа и защиты от несанкционированных действий. Проверять наличие, качество и анализировать достаточность оперативных средств самоконтроля системы защиты информации;
>• разработать тест-программу, организовать ее запуск и функционирование во время проведения специальных исследований;
>• инструментально-расчетным методом с использованием различной аппаратуры контроля определять источник и параметры опасного сигнала, выполнение в местах возможного размещения средств разведки норм защиты информации, обрабатываемой средствами информатики, и речевой информации, циркулирующей в выделенных помещениях, разведопасные направления для перехвата информации, влияние условий размещения средств информатики, прокладки их линий связи и других коммуникаций на объекте, окружающих предметов (металлоконструкций), а также расположения выделенных помещений на возможности перехвата информации в реальных условиях;
>• проверять возможность утечки информации по различным каналам, образующимся при обработке информации средствами информатики, и речевой информации, циркулирующей в выделенных помещениях, за счет неравномерностей потребления тока в цепях питания, электромагнитных наводок во вспомогательных коммуникациях, цепях заземления, других токопроводящих коммуникациях и металлоконструкциях, возникновения паразитных электроакустических преобразований и генерации в средствах информатики, распространения звуковых волн в различных средах;
>• эксплуатировать, готовить, проверять основные технические параметры штатной аппаратуры контроля, характеризующие ее готовность к работе. Калибровать аппаратуру контроля;
>• работать на персональных ЭВМ. С помощью специального программного обеспечения выполнять необходимые расчеты при обработке результатов контроля, работать с базами данных, готовить выходные (отчетные)

документы;
>• организовать ремонт, техническое обслуживание и поверку применяемой контрольно-измерительной аппаратуры, вычислительной и специальной техники.
1.3. Специалисты предприятий-заявителей должны ИМЕТЬ опыт практической работы по обеспечению защиты информации, обрабатываемой средствами информатики и циркулирующей в выделенных помещениях, и проверке эффективности мер защиты информации на объектах контроля.
2.1. Каждый определенный в заявке вид работ по защите информации должен быть обеспечен средствами измерений и контроля в объеме и по качеству достаточном для проведения, в соответствии с действующими на момент заявления методиками, измерений параметров технических средств, типы которых определены в заявлении. Допускается использование средств измерений на условиях аренды.
2.2. Измерительная база должна ОБЕСПЕЧИВАТЬ:
>• возможность проведения измерений полей в диапазоне частот, установленном в действующей методике (требования по диапазону частот);
>• возможность измерения уровней полей технических средств (требования по чувствительности);
>• возможность измерения опасных сигналов на фоне стационарных полей посторонних радиоэлектронных средств (требования по избирательности);
>• достоверность полученных значений полей (требования по точности, требования по динамическому диапазону);
>• возможность идентификации опасных излучений конкретному образцу, физической цепи (требования по идентификации).
Каждый тип средства измерений и контроля должен быть предназначен для проведения конкретных видов измерений (требования по назначению).
Средства измерений и контроля должны быть метрологически проверены (требования по метрологическому обеспечению).
При измерениях в цепях (средах), опасных для здоровья, должны быть предусмотрены пробники, съемники, датчики и средства защиты, обеспечивающие безопасность проведения работ.
3.1. Требования к помещениям, предназначенным для проведения измерений при предварительных и лабораторных специсследованиях (сертификации продукции), и их технической и технологической оснащенности рассматриваются как совокупность требований к разработанной технологии проведения измерений, измерительной аппаратуре, помещениям, стендам, антенным камерам, а также к организации их содержания, обслуживания и поверки, выполнение которых позволяет организации, претендующей на проведение работ, указанных в заявке, получить лицензию на право их проведения. Кроме того, на предприятии, претендующем на получение лицензии, должны быть выделены помещения, обеспечивающие сохранность исследуемых технических средств заказчика и документов.
4.1. В целях обеспечения сохранности материальных ценностей заказчика и его коммерческих и других секретов, а также обеспечения заявителя секретной нормативно-методической документацией у него должен быть предусмотрен режимно-секретный орган (орган обеспечения безопасности информации) и обеспечена надежная охрана. Допускается отсутствие у заявителя собственных указанных служб при условии обеспечения его услугами таких служб предприятием, у которого арендуются помещения.

**«КОНЦЕПЦИЯ ЗАЩИТЫ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ»**

**Руководящий документ Гостехкомиссии РФ**

**Принятые сокращения**

АС — автоматизированная система
КСЗ — комплекс средств защиты НСД — несанкционированный доступ
ОС — операционная система

ППП — пакет прикладных программ
ПРД — правила разграничения доступа
РД — руководящий документ
СВТ — средства вычислительной техники
СЗИ — система защита информации СЗИ
НСД — система защиты информации от несанкционированного доступа
СЗСИ — система защиты секретной информации
СНТП — специальное научно-техническое подразделение
СРД — система разграничения доступа
СУБД — система управления базами данных
ТЗ — техническое задание ЭВМ — электронно-вычислительная машина
ЭВТ — электронно-вычислительная техника

**1. Общие положения**

1.1. Настоящий документ излагает систему взглядов, основных принципов, которые закладываются в основу проблемы защиты информации от НСД, являющейся частью общей проблемы безопасности информации.

1.2. Концепция предназначена для заказчиков, разработчиков и пользователей СВТ и АС, которые используются для обработки, хранения и передачи требующей защиты информации.

1.3. Концепция является методологической базой нормативно-технических и методических документов, направленных на решение следующих задач:

>• выработка требований по защите СВТ и АС от НСД к информации;

>• создание защищенных от НСД к информации СВТ и АС;

>• сертификация защищенных СВТ и АС.

1.4. Концепция предусматривает существование двух относительно самостоятельных и, следовательно, имеющих отличие направлений в проблеме защиты информации от НСД: направление, связанное с СВТ, и направление, связанное с АС.

Отличие двух направлений порождено тем, что СВТ разрабатываются и поставляются на рынок лишь как элементы, из которых в дальнейшем строятся функционально ориентированные АС, и поэтому, не решая прикладных задач, СВТ не содержат пользовательской информации.

Помимо пользовательской информации при создании АС появляются такие отсутствующие при разработке СВТ характеристики АС, как полномочия пользователей, модель нарушителя, технология обработки информации.

В связи с этим, если понятия защищенность (защита) информации от НСД в АС и защищенность (защита) АС от НСД к информации эквивалентны, то в случае СВТ можно говорить лишь о защищенности (защите) СВТ от НСД к информации, для обработки, хранения и передачи которой оно предназначено.

При этом защищенность СВТ есть потенциальная защищенность, т.е. свойство предотвращать или существенно затруднять НСД к информации в дальнейшем при использовании СВТ в АС.

**2. Определение НСД**

2.1. При анализе общей проблемы безопасности информации выделяются те направления, в которых преднамеренная или непреднамеренная деятельность человека, а также неисправности технических средств, ошибки программного обеспечения или стихийные бедствия могут привести к утечке, модификации или уничтожению информации.

Известны такие направления исследования проблемы безопасности информации, как радиотехническое, побочные электромагнитные излучения и наводки, акустическое, НСД и др.

2.2. НСД определяется как доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых СВТ или АС.

Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения СВТ или АС.

**3. Основные принципы защиты от НСД**

3.1. Защита СВТ и АС основывается на положениях и требованиях существующих законов, стандартов и нормативно-методических документов по защите от НСД к информации.

3.2. Защита СВТ обеспечивается комплексом программно-технических средств.

3.3. Защита АС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер.

3.4. Защита АС должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

3.5. Программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики АС (надежность, быстродействие, возможность изменения конфигурации АС).

3.6. Неотъемлемой частью работ по защите является оценка эффективности средств защиты, осуществляемая по методике, учитывающей всю совокупность технических характеристик оцениваемого объекта, включая технические решения и практическую реализацию средств защиты.

3.7. Защита АС должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем АС или контролирующими органами.

**4. Модель нарушителя в АС**

4.1. В качестве нарушителя рассматривается субъект, имеющий доступ к работе со штатными средствами АС и СВТ как части АС.

Нарушители классифицируются по уровню возможностей, предоставляемых им штатными средствами АС и СВТ. Выделяется четыре уровня этих возможностей.

Классификация является иерархической, т. е. каждый следующий уровень включает в себя функциональные возможности предыдущего.

4.2. Первый уровень определяет самый низкий уровень возможностей ведения диалога в АС — запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации.

Второй уровень определяется возможностью создания и запуска собственных программ с новыми функциями по обработке информации.

Третий уровень определяется возможностью управления функционированием АС, т. е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования. Четвертый уровень определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС, вплоть до включения в состав СВТ собственных технических средств с новыми функциями по обработке информации.

4.3. В своем уровне нарушитель является специалистом высшей квалификации, знает все об АС и, в частности, о системе и средствах ее защиты.

**5. Основные способы НСД**

К основным способам НСД относятся:

>• непосредственное обращение к объектам доступа;

>• создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;

>• модификация средств защиты, позволяющая осуществить НСД;

>• внедрение в технические средства СВТ или АС программных или технических механизмов, нарушающих предполагаемую структуру и функции СВТ или АС и позволяющих осуществить НСД.

**6. Основные направления обеспечения защиты от НСД**

6.1. Обеспечение защиты СВТ и АС осуществляется:

СРД субъектов к объектам доступа;
обеспечивающими средствами для СРД.
6.2. Основными функциями СРД являются:
>• реализация ПРД субъектов и их процессов к данным;
>• реализация ПРД субъектов и их процессов к устройствам создания твердых копий;
>• изоляция программ процесса, выполняемого в интересах субъекта, от других субъектов;
>• управление потоками данных с целью предотвращения записи данных на носители несоответствующего грифа;
>• реализация правил обмена данными между субъектами для АС и СВТ, построенных по сетевым принципам.
**6.3.** Обеспечивающие средства для СРД выполняют следующие функции:
>• идентификацию и опознание (аутентификацию) субъектов и поддержание привязки субъекта к процессу, выполняемому для субъекта;
>• регистрацию действий субъекта и его процесса;
>• предоставление возможностей исключения и включения новых субъектов и объектов доступа, а также изменение полномочий субъектов;
>• реакцию на попытки НСД, например, сигнализацию, блокировку, восстановление после НСД;
>• тестирование;
>• очистку оперативной памяти и рабочих областей на магнитных носителях после завершения работы пользователя с защищаемыми данными;
>• учет выходных печатных и графических форм и твердых копий в АС;
>• контроль целостности программной и информационной части как СРД, так и обеспечивающих ее средств.
6.4. Ресурсы, связанные как с СРД, так и с обеспечивающими ее средствами, включаются в объекты доступа.
6.5. Способы реализации СРД зависят от конкретных особенностей СВТ и АС. Возможно применение следующих способов защиты и любых их сочетаний:
>• распределенная СРД и СРД, локализованная в программно-техническом комплексе (ядро защиты);
>• СРД в рамках операционной системы, СУБД или прикладных программ;
>• СРД в средствах реализации сетевых взаимодействий или на уровне приложений;
>• использование криптографических преобразований или методов непосредственного контроля доступа;
>• программная и (или) техническая реализация СРД.

**7. Основные характеристики технических средств защиты от НСД**

7.1. Основными характеристиками технических средств защиты **являются:**
>• степень полноты и качество охвата ПРД реализованной СРД;
>• состав и качество обеспечивающих средств для СРД;
>• гарантии правильности функционирования СРД и обеспечивающих ее средств.
7.2. Полнота и качество охвата ПРД оценивается по наличию четких непротиворечивых заложенных в СРД правил доступа к объектам доступа и мерам их надежной идентификации. Учитываются также возможности контроля разнообразных дисциплин доступа к данным.
7.3. При оценке состава и качества обеспечивающих средств для СРД учитываются средства идентификации и опознания субъектов и порядок их использования, полнота учета действий субъектов и способы поддержания привязки субъекта к его процессу.
7.4. Гарантии правильности функционирования оцениваются по способам проектирования и реализации СРД и обеспечивающих ее средств (формальная и неформальная верификация) и по составу и качеству препятствующих обходу СРД средств (поддержание целостности СРД и обеспечивающих средств, восстановление после сбоев, отказов и попыток НСД, контроль

дистрибуций, возможность тестирования на этапе эксплуатации).
7.5. Оцениваемые АС или СВТ должны быть тщательно документированы. В состав документации включаются Руководство пользователя по использованию защитных механизмов и Руководство по управлению средствами защиты. Для АС и СВТ, претендующих на высокий уровень защищенности, оценка осуществляется при наличии проектной документации (эскизный, технический и рабочий проекты), а также описаний процедур тестирования и их результатов.

**8. Классификация АС**

8.1. Классификация необходима для более детальной, дифференцированной разработки требований по защите от НСД с учетом специфических особенностей этих систем.
8.2. В основу системы классификации АС должны быть положены следующие характеристики объектов и субъектов защиты, а также способов их взаимодействия:
>• информационные, определяющие ценность информации, ее объем и степень (гриф) конфиденциальности, а также возможные последствия неправильного функционирования АС и>•за искажения (потери) информации;
>• организационные, определяющие полномочия пользователей;
>• технологические, определяющие условия обработки информации, например, способ обработки (автономный, мультипрограммный и т. д.), время циркуляции (транзит, хранение и т. д.), вид АС (автономная, сеть, стационарная, подвижная и т. д.).

**9. Организация работ по защите от НСД**

9.1. Организация работ по защите СВТ и АС от НСД к информации должна быть частью общей организации работ по безопасности информации.
9.2. Обеспечение защиты основывается на требованиях по защите к разрабатываемым СВТ и АС, формулируемых заказчиком и согласуемых с разработчиком.
Эти требования задаются либо в виде желаемого уровня защищенности СВТ или АС, либо в виде определенного, соответствующего этому уровню перечня требований.
Требования по защите обеспечиваются разработчиком в виде комплекса средств защиты. Организационные мероприятия для АС реализуются заказчиком.
Ответственность за разработку КСЗ возлагается на главного конструктора СВТ или АС.
9.3. Проверка выполнения технических требований по защите проводится аналогично с другими техническими требованиями в процессе испытаний (предварительных, государственных и др.).
По результатам успешных испытаний оформляется документ (сертификат), удостоверяющий соответствие СВТ или АС требованиям по защите и дающий право разработчику на использование и (или) распространение их как защищенных.
9.4. Разработка мероприятий по защите должна проводиться одновременно с разработкой СВТ и АС и выполняться за счет финансовых и материально-технических средств (ресурсов), выделенных на разработку СВТ и АС.

**«АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ. КЛАССИФИКАЦИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ И ТРЕБОВАНИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ»**

**Руководящий документ Гостехкомиссии РФ**

Настоящий руководящий документ устанавливает классификацию автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в АС различных классов.
Руководящий документ разработан в дополнение ГОСТ 34.003-90, ГОСТ 34.601-90, РД 50-680-88, РД 50-34.680-90 и других документов.

Документ может использоваться как нормативно-методический материал для заказчиков и разработчиков АС при формулировании и реализации требований по защите.

**Принятые сокращения**

АС — автоматизированные системы НСД — несанкционированный доступ
РД — руководящий документ СЗИ — система защиты информации
СЗИ НСД — система защиты информации от несанкционированного доступа

**1. Классификация АС**

1.1. Классификация распространяется на все действующие и проектируемые АС учреждений, организаций и предприятий, обрабатывающие конфиденциальную информацию.

1.2. Деление АС на соответствующие классы по условиям их функционирования с точки зрения защиты информации необходимо в целях разработки и применения обоснованных мер по достижению требуемого уровня защиты информации.

1.3. Дифференциация подхода к выбору методов и средств защиты определяется важностью обрабатываемой информации, различием АС по своему составу, структуре, способам обработки информации, количественному и качественному составу пользователей и обслуживающего персонала.

1.4. Основными этапами классификации АС являются:

>• разработка и анализ исходных данных;
>• выявление основных признаков АС, необходимых для классификации;
>• сравнение выявленных признаков АС с классифицируемыми;
>• присвоение АС соответствующего класса защиты информации от НСД.

1.5. Необходимыми исходными данными для проведения классификации конкретной АС являются:

>• перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности;
>• перечень лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий;
>• матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС;
>• режим обработки данных в АС.

1.6. Выбор класса АС производится заказчиком и разработчиком с привлечением специалистов по защите информации.

1.7. К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

>• наличие в АС информации различного уровня конфиденциальности;
>• уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;
>• режим обработки данных в АС — коллективный или индивидуальный.

1.8. Устанавливается девять классов защищенности АС от НСД к информации.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите.

Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС.

В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

1.9. Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса — 3Б и 3А.

Вторая группа включает АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности.

Группа содержит два класса — 2Б и 2А.
Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов — 1Д, 1Г, 1В, 1Б и 1А.

**2. Требования по защите информации от НСД для АС**

2.1. Защита информации от НСД является составной частью общей проблемы обеспечения безопасности информации. Мероприятия по защите информации от НСД должны осуществляться взаимосвязано с мероприятиями по специальной защите основных и вспомогательных средств вычислительной техники, средств и систем связи от технических средств разведки и промышленного шпионажа.

2.2. В общем случае, комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД реализуется в рамках системы защиты информации от НСД (СЗИ НСД), условно состоящей из следующих четырех подсистем:

>• управления доступом;
>• регистрации и учета;
**>•** криптографической;
>• обеспечения целостности.

2.3. В зависимости от класса АС в рамках этих подсистем должны быть реализованы требования в соответствии с пп. 2.4, 2.7 и 2.10. Подробно эти требования сформулированы в пп. 2.5, 2.6, 2.8, 2.9 и 2.11—2.15.

2.4. Требования к АС третьей группы.

Подсистемы и требования /Классы
/ЗБ /ЗА
1. Подсистема управления доступом / /
1.1. Идентификация, проверка подлинности и контроль доступа субъектов: / /
>• в систему /+ /+
>• к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ /- /-
>• к программам /— /—
>• к томам, каталогам, файлам, записям, полям записей /— /—
1.2. Управление потоками информации /— /—
2. Подсистема регистрации и учета / /
2.1. Регистрация и учет: / /

Окончание табл.

Подсистемы и требования /Классы
/ЗБ/ЗА
>• входа (выхода) субъектов доступа в (из) системы (узел сети) /+ /+
>•выдачи печатных (графических) выходных документов /- /+
>• запуска (завершения) программ и процессов (заданий, задач) /- /-
>• доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи /— /-
>•доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей/ /
>• изменения полномочий субъектов доступа /- /-
>• создаваемых защищаемых объектов доступа /— /—
2.2. Учет носителей информации /+ /+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей /— /+
2.4. Сигнализация попыток нарушения защиты /— /—

3. Криптографическая подсистема / /
3.1. Шифрование конфиденциальной информации /- /-
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах /— /-
3.3. Использование аттестованных (сертифицированных) криптографических средств /— /—
4. Подсистема обеспечения целостности / /
4.1. Обеспечение целостности программных средств и обрабатываемой информации /+ /+
4.2. Физическая охрана средств вычислительной техники и носителей информации /+ /+
4.3. Наличие администратора (службы) защиты информации в АС, /- /-
4.4. Периодическое тестирование СЗИ НСД /+ /+
4.5. Наличие средств восстановления СЗИ НСД /+ /+
4.6. Использование сертифицированных средств защиты /- /+
Обозначения:
«-» — нет требований к данному классу;
«+» — есть требования к данному классу.
2.5. Требования к классу защищенности 3Б:
Подсистема управления доступом:
>• должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов.
Подсистема регистрации и учета:
>• должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:
• дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
• должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку). Подсистема обеспечения целостности:
>• должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды. При этом:
• целостность СЗИ НСД проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗИ;
• целостность программной среды обеспечивается отсутствием в АС. средств разработки и отладки программ;
>• должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;
>• должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД;
>• должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.
2.6. Требования к классу защищенности 3А:
Подсистема управления доступом:
>• должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия

длиной не менее шести буквенно-цифровых символов.
Подсистема регистрации и учета:
>• должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:
• дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
• результат попытки входа: успешная или неуспешная (при НСД);
>• должна осуществляться регистрация выдачи печатных (графических) документов на «твердую» копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа порядковым номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц). В параметрах регистрации указываются:
• дата и время выдачи (обращения к подсистеме вывода);
• краткое содержание документа (наименование, вид, код, шифр) и уровень его конфиденциальности;
• спецификация устройства выдачи [логическое имя (номер) внешнего устройства];
**>•** должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);
>• должно проводиться несколько видов учета (дублирующих) с регистрацией выдачи (приема) носителей информации;
>• должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).
Подсистема обеспечения целостности:
>• должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды. При этом:
• целостность СЗИ НСД проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗИ;
• целостность программной среды обеспечивается отсутствием в АС средств разработки и отладки программ;
>• должны осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС;
>• должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД;
**>•** должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновлением контроль работоспособности;
**>•** должны использоваться сертифицированные средства защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации средств защиты СЗИ НСД. 2.7. Требования к АС второй группы.
Подсистемы и требования /Классы
/2Б /2А

1. Подсистема управления доступом / /
1.1. Идентификация, проверка подлинности и контроль доступа / /
>•субъектов: /+ /+
>• систему /— /+
>• терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ /- /+
>• к программам /— /+
>• томам, каталогам, файлам, записям, полям записей /- /+
1.2. Управление потоками информации /+ /+
2. Подсистема регистрации и учета / /
2.1. Регистрация и учет: / /
>• входа (выхода) субъектов доступа в (из) систему (узел сети) /— /+
>• выдачи печатных (графических) выходных документов /— /+
>• запуска (завершения) программ и процессов (заданий, задач) /— /+
>• доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи /- /+
>• доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей /- /-
>• изменения полномочий субъектов доступа создаваемых защищаемых объектов доступа /- /+
2.2. Учет носителей информации /+ /+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей /- /+
2.4. Сигнализация попыток нарушения защиты /— /—
3. Криптографическая подсистема / /
3.1. Шифрование конфиденциальной информации /— /+
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах /- /——
3.3. Использование аттестованных (сертифицированных) криптографических средств / /+
4. Подсистема обеспечения целостности / /
4.1. Обеспечение целостности программных средств и обрабатываемой информации /+ /+
4.2. Физическая охрана средств вычислительной техники и носителей информации /+ /+
4.3. Наличие администратора (службы) защиты информации в АС/— /+
Окончание табл.
Подсистемы и требования /Классы
/2Б /2А
4.4. Периодическое тестирование СЗИ НСД /+ /+
4.5. Наличие средств восстановления СЗИ НСД /+ /+
4.6. Использование сертифицированных средств защиты /— /+
Обозначения:
«-» — нет требований к данному классу;
«+» —есть требования к данному классу.
2.8. Требования к классу защищенности 2Б:
Подсистема управления доступом:
>• должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.
Подсистема регистрации и учета:
>• должна осуществляться регистрация входа (выхода) субъектов доступа в

систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:
• дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
• результат попытки входа: успешная или неуспешная (при НСД);
>• должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (карточку). Подсистема обеспечения целостности:
>• должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды. При этом:
• целостность СЗИ НСД проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗИ;
• целостность программной среды обеспечивается отсутствием в АС средств разработки и отладки программ во время обработки и (или) хранения защищаемой информации;
>• должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;
**>•** должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД;
>• должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.
2.9. Требования к классу защищенности 2А.
Подсистема управления доступом:
>• должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;
>• должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по их логическим адресам (номерам);
>• должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;
>• должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на них информации.
Подсистема регистрации и учета:
>• должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:
• дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
• результат попытки входа: успешная или неуспешная (при НСД);
• идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
>• должна осуществляться регистрация выдачи печатных (графических) документов на «твердую» копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа

порядковым номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц). В параметрах регистрации указываются:
• дата и время выдачи (обращения к подсистеме вывода);
• спецификация устройства выдачи [логическое имя (номер) внешнего устройства], краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;
• идентификатор субъекта доступа, запросившего документ;
>• должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются:
• дата и время запуска;
• имя (идентификатор) программы (процесса, задания);
• идентификатор субъекта доступа, запросившего программу (процесс, задание);
• результат запуска (успешный, неуспешный — несанкционированный);
>• должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:
• дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная — несанкционированная,
• идентификатор субъекта доступа;
• спецификация защищаемого файла;
>• должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:
• дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная — несанкционированная;
• идентификатор субъекта доступа;
• спецификация защищаемого объекта [логическое имя (номер)];
**>•** должен осуществляться автоматический учет создаваемых защищаемых файлов с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта;
>• должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);
>• учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема);
>• должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации;
>• должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).
Криптографическая подсистема:
>• должно осуществляться шифрование всей конфиденциальной информации, записываемой на совместно используемые различными субъектами доступа (разделяемые) носители данных, в каналах связи, а также на съемные носители данных (дискеты, микрокассеты и т. п.) долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа. При этом должны выполняться автоматическое освобождение и очистка областей внешней памяти, содержавших ранее незашифрованную информацию;

>• доступ субъектов к операциям шифрования и криптографическим ключам должен дополнительно контролироваться подсистемой управления доступом;
>• должны использоваться сертифицированные средства криптографической защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации криптографических средств защиты.
Подсистема обеспечения целостности:
>• должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды. При этом:
• целостность СЗИ НСД проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗИ;
• целостность программной среды обеспечивается отсутствием в АС средств разработки и отладки программ;
>• должны осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС;
>• должен быть предусмотрен администратор (служба) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы СЗИ НСД;
>• должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД;
>• должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности;
>• должны использоваться сертифицированные средства защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации средств защиты СЗИ НСД.
2.10. Требования к АС первой группы.
Подсистемы и требования /Классы
/1Д /1Г /1В /1Б /1А
1. Подсистема управления доступом /— /— /+ /+ /+
1.1. Идентификация, проверка подлинности и контроль доступа субъектов: / / / / /
>• в систему / / / / /
>• к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ / / / / /
>• к программам / / / / /
>• к томам, каталогам, файлам, записям, полям записей / / / / /
1.2. Управление потоками информации / / / / /
2. Подсистема регистрации и учета / / / / /
2.1. Регистрация и учет / / / / /
>• входа (выхода) субъектов доступа в (из) систему (узел сети) / / / / /
>• выдачи печатных (графических) выходных документов / / / / /
>• запуска (завершения) программ и процессов (заданий, задач) / / / / /
>• доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи / / / / /
>• доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей / / / / /

>• изменения полномочий субъектов доступа создаваемых защищаемых объектов доступа / / / / /
2.2. Учет носителей информации / / / / /
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей / / / / /
2.4. Сигнализация попыток нарушения защиты / / / / /
3. Криптографическая подсистема / / / / /
3.1. Шифрование конфиденциальной информации / / / / /
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах / / / / /
3.3. Использование аттестованных (сертифицированных) криптографических средств / / / / /
4. Подсистема обеспечения целостности / / / / /
4.1. Обеспечение целостности программных средств и обрабатываемой информации/ / / / /
Окончание табл.
Подсистемы и требования /Классы
/1Д /1Г /1В /1Б /1А
4.2. Физическая охрана средств вычислительной техники и носителей информации /- /- /+ /+ /+
4.3. Наличие администратора (службы защиты информации в АС / / / / /
4.4. Периодическое тестирование СЗИ НСД / / / / /
4.5. Наличие средств восстановления СЗИ НСД / / / / /
4.6. Использование сертифицированных средств защиты / / / / /
Обозначения:
« — » — нет требований к данному классу;
« + » — есть требования к данному классу.
2.11. Требования к классу защищенности 1Д:
Подсистема управления доступом:
>• должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.
Подсистема регистрации и учета:
>• должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:
• дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
• результат попытки входа: успешная или неуспешная — несанкционированная;
• идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
>• должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных журнал (учетную карточку);
>• учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема).
Подсистема обеспечения целостности:
>• должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды. При этом:
• целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ;

• целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации;
>• должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;
**>•** должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД;
>• должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.
2.12. Требования к классу защищенности 1Г:
Подсистема управления доступом:
>• должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;
>• должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по логическим именам;
**>•** должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;
>• должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа.
Подсистема регистрации и учета:
>• должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:
• дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
• результат попытки входа: успешная или неуспешная — несанкционированная;
• идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
• код или пароль, предъявленный при неуспешной попытке;
>• должна осуществляться регистрация выдачи печатных (графических) документов на «твердую» копию. В параметрах регистрации указываются:
• дата и время выдачи (обращения к подсистеме вывода);
• спецификация устройства выдачи [логическое имя (номер) внешнего устройства];
• краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;
• идентификатор субъекта доступа, запросившего документ;
>• должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются:
• дата и время запуска;
• имя (идентификатор) программы (процесса, задания);
• идентификатор субъекта доступа, запросившего программу (процесс, задание);
• результат запуска (успешный, неуспешный — несанкционированный);
**>•** должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В

параметрах регистрации указываются:
• дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная — несанкционированная;
• идентификатор субъекта доступа;
• спецификация защищаемого файла;
>• должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:
• дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная — несанкционированная;
• идентификатор субъекта доступа;
• спецификация защищаемого объекта [логическое имя (номер)];
**>•** должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);
**>•** учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема);
>• должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется однократной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов);
Подсистема обеспечения целостности:
>• должна быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды. При этом:
• целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ;
• целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;
>• должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД;
>• должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности. 2.13. Требования к классу защищенности 1В:
Подсистема управления доступом:
>• должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;
**>•** должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по логическим именам и (или) адресам;
>• должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;
>• должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа;
**>•** должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей

должен быть не ниже уровня конфиденциальности записываемой на него информации. Подсистема регистрации и учета:
>• должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:
• дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
• результат попытки входа: успешная или неуспешная — несанкционированная;
• идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
• код или пароль, предъявленный при неуспешной попытке;
>• должна осуществляться регистрация выдачи печатных (графических) документов на «твердую» копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа его последовательным номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц). В параметрах регистрации указываются:
• дата и время выдачи (обращение к подсистеме вывода);
• спецификация устройства выдачи [логическое имя (номер) внешнего устройства];
• краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;
• идентификатор субъекта доступа, запросившего документ;
• объем фактически выданного документа (количество страниц, листов, копий) и результат выдачи: успешный (весь объем), неуспешный;
>• должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются:
• дата и время запуска;
• имя (идентификатор) программы (процесса, задания);
• идентификатор субъекта доступа, запросившего программу (процесс, задание);
• результат запуска (успешный, неуспешный — несанкционированный);
>• должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:
• дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная — несанкционированная;
• идентификатор субъекта доступа;
• спецификация защищаемого файла;
• имя программы (процесса, задания, задачи), осуществляющей доступ к файлу;
• вид запрашиваемой операции (чтение, запись, удаление, выполнение, расширение и т. п.);
>• должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:
• дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная — несанкционированная;
• идентификатор субъекта доступа;
• спецификация защищаемого объекта [логическое имя (номер)];
• имя программы (процесса, задания, задачи), осуществляющей доступ к

защищаемому объекту;
• вид запрашиваемой операции (чтение, запись, монтирование, захват и т. п.);
>• должна осуществляться регистрация изменений полномочий субъектов доступа и статуса объектов доступа. В параметрах регистрации указываются:
• дата и время изменения полномочий;
• идентификатор субъекта доступа (администратора), осуществившего изменения;
>• должен осуществляться автоматический учет создаваемых защищаемых файлов с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта;
>• должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и занесением учетных данных в журнал (учетную карточку);
>• учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема);
>• должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации;
>• должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в любую освобождаемую область памяти, использованную для хранения защищаемой информации;
>• должна осуществляться сигнализация попыток нарушения защиты.
Подсистема обеспечения целостности:
>• должна быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды. При этом:
• целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ;
• целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ при обработке и (или) хранении защищаемой информации;
• должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС;
>• должен быть предусмотрен администратор (служба) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы СЗИ НСД. Администратор должен иметь свой терминал и необходимые средства оперативного контроля и воздействия на безопасность АС;
>• должно проводиться периодическое тестирование всех функций СЗИ НСД с помощью специальных программных средств не реже одного раза в год;
>• должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности;
>• должны использоваться сертифицированные средства защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации средств защиты СЗИ НСД.
2.14. Требования к классу защищенности 1Б:
Подсистема управления доступом:
>• должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю

временного действия длиной не менее восьми буквенно-цифровых символов;
>• должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по физическим адресам (номерам);
>• должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;
>• должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа;
>• должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на него информации.
Подсистема регистрации и учета:
>• должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:
• дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
• результат попытки входа: успешный или неуспешный — несанкционированный;
• идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
• код или пароль, предъявленный при неуспешной попытке;
>• должна осуществляться регистрация выдачи печатных (графических) документов на «твердую» копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа его последовательным номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц). Вместе с выдачей документа должна автоматически оформляться учетная карточка документа с указанием даты выдачи документа, учетных реквизитов документа, краткого содержания (наименования, вида, шифра, кода) и уровня конфиденциальности документа, фамилии лица, выдавшего документ, количества страниц и копий документа (при неполной выдаче документа — фактически выданного количества листов в графе «Брак»). В параметрах регистрации указываются:
• дата и время выдачи (обращения к подсистеме вывода);
спецификация устройства выдачи [логическое имя (номер) внешнего устройства];
• краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;
• идентификатор субъекта доступа, запросившего документ;
• объем фактически выданного документа (количество страниц, листов, копий) и результат выдачи успешный (весь объем), неуспешный;
>• должна осуществляться регистрация запуска (завершения) всех программ и процессов (заданий, задач) в АС. В параметрах регистрации указываются:
• дата и время запуска;
• имя (идентификатор) программы (процесса, задания);
• идентификатор субъекта доступа, запросившего программу (процесс, задание);
• результат запуска (успешный, неуспешный — несанкционированный);
>• должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:
• дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная — несанкционированная;

• идентификатор субъекта доступа;
• спецификация защищаемого файла;
• имя программы (процесса, задания, задачи), осуществляющей доступ к файлу;
• вид запрашиваемой операции (чтение, запись, удаление, выполнение, расширение и т. п.);
>• должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:
• дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная — несанкционированная;
• идентификатор субъекта доступа;
• спецификация защищаемого объекта [логическое имя (номер)];
• имя программы (процесса, задания, задачи), осуществляющей доступ к защищаемому объекту;
• вид запрашиваемой операции (чтение, запись, монтирование, захват и т. п.);
>• должна осуществляться регистрация изменений полномочий субъектов доступа и статуса объектов доступа. В параметрах регистрации указываются:
• дата и время изменения полномочий;
• идентификатор субъекта доступа (администратора), осуществившего изменения;
• идентификатор субъекта, у которого проведено изменение полномочий и вид изменения (пароль, код, профиль и т. п.);
• спецификация объекта, у которого проведено изменение статуса защиты и вид изменения (код защиты, уровень конфиденциальности);
>• должен осуществляться автоматический учет создаваемых защищаемых файлов, инициируемых защищаемых томов, каталогов, областей оперативной памяти ЭВМ, выделяемых для обработки защищаемых файлов, внешних устройств ЭВМ, каналов связи, ЭВМ, узлов сети ЭВМ, фрагментов сети с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта;
>• должен проводиться учет всех защищаемых носителей информации с помощью их маркировки;
>• учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема);
>• должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации;
>• должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в любую освобождаемую область памяти, использованную для хранения защищаемой информации;
>• должна осуществляться сигнализация попыток нарушения защиты на терминал администратора и нарушителя.
Криптографическая подсистема:
>• должна осуществляться шифрование всей конфиденциальной информации, записываемой на совместно используемые различными субъектами доступа (разделяемые) носители данных, в каналах связи, а также на съемные портативные носители данных (дискеты, микрокассеты и т. п.) долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа. При этом должна выполняться принудительная очистка областей внешней памяти, содержавших ранее

незашифрованную информацию;
>• доступ субъектов к операциям шифрования и к соответствующим криптографическим ключам должен дополнительно контролироваться посредством подсистемы управления доступом;
>• должны использоваться сертифицированные средства криптографической защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации криптографических средств защиты.
Подсистема обеспечения целостности:
>• должна быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды. При этом:
>• целостность СЗИ НСД проверяется по контрольным суммам всех компонент СЗИ как в процессе загрузки, так и динамически в процессе работы АС;
>• целостность программной среды обеспечивается качеством приемки программных средств в АС, предназначенных для обработки защищенных файлов;
>• должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС;
>• должен быть предусмотрен администратор (служба) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы СЗИ НСД. Администратор должен иметь свой терминал и необходимые средства оперативного контроля и воздействия на безопасность АС;
>• должно проводиться периодическое тестирование всех функций СЗИ НСД с помощью специальных программных средств не реже одного раза в квартал;
>• должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности, а также оперативное восстановление функций СЗИ НСД при сбоях;
>• должны использоваться сертифицированные средства защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации средств защиты СЗИ НСД.
2.15. Требования к классу защищенности 1А:
Подсистема управления доступом:
>• должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по биометрическим характеристикам или специальным устройствам (жетонам, картам, электронным ключам) и паролю временного действия длиной не менее восьми буквенно-цифровых символов;
>• должна осуществляться аппаратурная идентификация и проверка подлинности терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по уникальным встроенным устройствам;
>• должна осуществляться идентификация и проверка подлинности программ, томов, каталогов, файлов, записей, полей записей по именам и контрольным суммам (паролям, ключам);
>• должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа;
>• должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на него информации.
Подсистема регистрации и учета:
>• должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из

системы или останов не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:
• дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
• результат попытки входа: успешная или неуспешная — несанкционированная;
• идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
• код или пароль, предъявленный при неуспешной попытке;
>• должна осуществляться регистрация выдачи печатных (графических) документов на «твердую» копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа его последовательным номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц). Вместе с выдачей документа должна автоматически оформляться учетная карточка документа с указанием даты выдачи документа, учетных реквизитов документа, краткого содержания (наименования, вида, шифра, кода) и уровня конфиденциальности документа, фамилии лица, выдавшего документ, количества страниц и копий документа (при неполной выдаче документа — фактически выданного количества листов в графе «Брак»). В параметрах регистрации указываются:
• дата и время выдачи (обращения к подсистеме вывода);
• спецификация устройства выдачи [логическое имя (номер) внешнего устройства];
• краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;
• идентификатор субъекта доступа, запросившего документ;
• объем фактически выданного документа (количество страниц, листов, копий) и результат выдачи: успешный (весь объем), неуспешный;
>• должна осуществляться регистрация запуска (завершения) всех программ и процессов (заданий, задач) в АС. В параметрах регистрации указываются:
• дата и время запуска;
• имя (идентификатор) программы (процесса, задания);
• идентификатор субъекта доступа, запросившего программу (процесс, задание);
• результат запуска (успешный, неуспешный — несанкционированный);
• полная спецификация соответствующего файла «образа» программы (процесса, задания) — устройство (том, каталог), имя файла (расширение);
>• должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:
• дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная — несанкционированная;
• идентификатор субъекта доступа;
• спецификация защищаемого файла;
• имя программы (процесса, задания, задачи), осуществляющей доступ к файлу, вид запрашиваемой операции (чтение, запись, удаление, выполнение, расширение и т. п.);
>• должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:
• дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная — несанкционированная;

• идентификатор субъекта доступа;
• спецификация защищаемого объекта [логическое имя (номер)];
• имя программы (процесса, задания, задачи), осуществляющей доступ к защищаемому объекту;
• вид запрашиваемой операции (чтение, запись, монтирование, захват и т.п.);
>• должна осуществляться регистрация изменений полномочий субъектов доступа и статуса объектов доступа. В параметрах регистрации указываются:
• дата и время изменения полномочий и статуса;
• идентификатор субъекта доступа (администратора), осуществившего изменения;
• идентификатор субъекта доступа, у которого изменены полномочия и вид изменений (пароль, код, профиль и т.п.);
• спецификация объекта, у которого изменен статус защиты, и вид изменения (код защиты, уровень конфиденциальности);
>• должен осуществляться автоматический учет создаваемых защищаемых файлов, инициируемых защищаемых томов, каталогов, областей оперативной памяти ЭВМ, выделяемых для обработки защищаемых файлов, внешних устройств ЭВМ, каналов связи, ЭВМ, узлов сети ЭВМ, фрагментов сети с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта;
>• должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);
>• учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема);
>• должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации;
>• должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в любую освобождаемую область памяти, в которой содержалась защищаемая информация;
>• должна осуществляться надежная сигнализация попыток нарушения защиты на терминал администратора и нарушителя.
Криптографическая подсистема:
>• должно осуществляться шифрование всей конфиденциальной информации, записываемой на совместно используемые различными субъектами доступа (разделяемые) носители данных, в каналах связи, а также на любые съемные носители данных (дискеты, микрокассеты и т. п.) долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа. При этом должна выполняться автоматическая очистка областей внешней памяти, содержавших ранее незашифрованную информацию;
>• должны использоваться разные криптографические ключи для шифрования информации, принадлежащей различным субъектам доступа (группам субъектов);
>• доступ субъектов к операциям шифрования и к соответствующим криптографическим ключам должен дополнительно контролироваться посредством подсистемы управления доступом;
>• должны использоваться сертифицированные средства криптографической защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации криптографических средств защиты.
Подсистема обеспечения целостности:

>• должна быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды. При этом:
• целостность СЗИ НСД проверяется по имитовставкам алгоритма ГОСТ 28147-89 или по контрольным суммам другого аттестованного алгоритма всех компонент СЗИ как в процессе загрузки, так и динамически в процессе функционирования АС;
• целостность программной среды обеспечивается качеством приемки любых программных средств в АС;
>• должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС;
>• должен быть предусмотрен администратор (служба) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы СЗИ НСД. Администратор должен иметь свой терминал и необходимые средства оперативного контроля и воздействия на безопасность АС;
>• должно проводиться периодическое тестирование всех функций СЗИ НСД с помощью специальных программных средств не реже одного раза в квартал;
>• должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности, а также автоматическое оперативное восстановление функций СЗИ НСД при сбоях;
>• должны использоваться сертифицированные средства защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации средств защиты СЗИ НСД.
2.16. Организационные мероприятия в рамках СЗИ НСД в АС, обрабатывающих или хранящих информацию, являющуюся собственностью государства и отнесенную к категории секретной, должны отвечать государственным требованиям по обеспечению режима секретности проводимых работ.
2.17. При обработке или хранении в АС информации, не отнесенной к категории секретной, в рамках СЗИ НСД государственным, коллективным, частным и совместным предприятиям, а также частным лицам рекомендуются следующие организационные мероприятия:
>• выявление конфиденциальной информации и ее документальное оформление в виде перечня сведений, подлежащих защите;
>• определение порядка установления уровня полномочий субъекта доступа, а также круга лиц, которым это право предоставлено;
>• установление и оформление правил разграничения доступа, т.е. совокупности правил, регламентирующих права доступа субъектов к объектам;
>• ознакомление субъекта доступа с перечнем защищаемых сведений и его уровнем полномочий, а также с организационно-распорядительной и рабочей документацией, определяющей требования и порядок обработки конфиденциальной информации;
>• получение от субъекта доступа расписки о неразглашении доверенной ему конфиденциальной информации;
>• обеспечение охраны объекта, на котором расположена защищаемая АС, (территория, здания, помещения, хранилища информационных носителей) путем установления соответствующих постов, технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими хищение средств вычислительной техники (СВТ), информационных носителей, а также НСД к СВТ и линиям связи;
>• выбор класса защищенности АС в соответствии с особенностями обработки информации (технология обработки, конкретные условия эксплуатации АС) и уровнем ее конфиденциальности;

>• организация службы безопасности информации (ответственные лица, администратор АС), осуществляющей учет, хранение и выдачу информационных носителей, паролей, ключей, ведение служебной информации СЗИ НСД (генерацию паролей, ключей, сопровождение правил разграничения доступа), приемку включаемых в АС новых программных средств, а также контроль за ходом технологического процесса обработки конфиденциальной информации и т. д.;
>• разработка СЗИ НСД, включая соответствующую организационно-распорядительную и эксплуатационную документацию;
>• осуществление приемки СЗИ НСД в составе АС.
2.18. При разработке АС, предназначенной для обработки или хранения информации, являющейся собственностью государства и отнесенной к категории секретной, необходимо ориентироваться в соответствии с РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» на классы защищенности АС не ниже (по группам) ЗА, 2А, 1А, 1Б, 1В и использовать сертифицированные СВТ:
>• не ниже 4-го класса — для класса защищенности АС 1В;
>• не ниже 3-го класса — для класса защищенности АС 1Б;
>• не ниже 2-го класса — для класса защищенности АС 1А.

**«СРЕДСТВА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ. ЗАЩИТА ОТ НСД К ИНФОРМАЦИИ. ПОКАЗАТЕЛИ ЗАЩИЩЕННОСТИ ОТ НСД К ИНФОРМАЦИИ» Руководящий документ Гостехкомиссии РФ**

Настоящий Руководящий документ устанавливает классификацию средств вычислительной техники по уровню защищенности от несанкционированного доступа к информации на базе перечня показателей защищенности и совокупности описывающих их требований.
Под СВТ понимается совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

**Принятые сокращения**

АС — автоматизированная система
КД — конструкторская документация
КСЗ — комплекс средств защиты
НСД — несанкционированный доступ
ПРД — правила разграничения доступа
СВТ — средства вычислительной техники

**1. Общие положения**

1.1. Данные показатели содержат требования защищенности СВТ от НСД к информации.
1.2. Показатели защищенности СВТ применяются к общесистемным программным средствам и операционным системам (с учетом архитектуры ЭВМ).
Конкретные перечни показателей определяют классы защищенности СВТ. Уменьшение или изменение перечня показателей, соответствующего конкретному классу защищенности СВТ, не допускается.
Каждый показатель описывается совокупностью требований. Дополнительные требования к показателю защищенности СВТ и соответствие этим дополнительным требованиям оговаривается особо.
1.3. Требования к показателям реализуются с помощью программно-технических средств.
Совокупность всех средств защиты составляет комплекс средств защиты. Документация КСЗ должна быть неотъемлемой частью конструкторской документации на СВТ.
1.4. Устанавливается семь классов защищенности СВТ от НСД к информации. Самый низкий класс — седьмой, самый высокий — первый.
Классы подразделяются на четыре группы, отличающиеся качественным

уровнем защиты:
>• первая группа содержит только один седьмой класс;
**>•** вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;
>• третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;
>• четвертая группа характеризуется верифицированной защитой и содержит только первый класс.
1.5. Выбор класса защищенности СВТ для автоматизированных систем, создаваемых на базе защищенных СВТ, зависит от грифа секретности обрабатываемой в АС информации, условий эксплуатации и расположения объектов системы.
1.6. Применение в комплекте СВТ средств криптографической защиты информации по ГОСТ 28147-89 может быть использовано для повышения гарантий качества защиты.

**2. Требования к показателям защищенности**

2.1. Показатели защищенности
2.1.1. Перечень показателей по классам защищенности СВТ приведен в таблице.

Показатель защищенности /Класс защищенности
/6 /5 /4 /3 /2 /1
Дискреционный принцип контроля доступа /+ /+ /+ /= /+ /=
Мандатный принцип контроля доступа /— /— /+ /= /= /=
Очистка памяти /— /+ /+ /+ /= /=
Изоляция модулей /— /— /+ /= /+ /=
Маркировка документов /— /— /+ /= /= /=
Защита ввода и вывода на отчуждаемый физический носитель информации /~ / /+ /— /=/=
Сопоставление пользователя с устройством /- /— /+ /= /= /=
Идентификация и аутентификация /+ /= /+ /= /= /=
Гарантии проектирования /- /+ /+ /+ /+ /+
Регистрация /— /+ /+ /+ /= /=
Взаимодействие пользователя с СЗ /— /— /— /+ /= /=
Надежное восстановление /— /— /— /+ /= /=
Целостность СЗ /— /+ /+ /+ /= /=

Окончание табл.

Показатель защищенности /Класс защищенности
/6 /5 /4 /3 /2 /1
Контроль модификации /- /- /- /— /+ /=
Контроль дистрибуции /— /— /— /- /+ /=
Гарантии архитектуры /— /— /— /— /- /+
Тестирование /+ /+ /+ /+ /+ /=
Руководство для пользователя /+ /= /= /= /= /=
Руководство по СЗ /+ /+ /= /+ /+ /=
Тестовая документация /+ /+ /+ /+ /+ /=
Конструкторская (проектная) документация /+ /+ /+ /+ /+ /+

Обозначения:
«-» — нет требований к данному классу;
«+» — новые или дополнительные требования,
«=» — требования совпадают с требованиями к СВТ предыдущего класса.
2.1.2. Приведенные в данном разделе наборы требований к показателям каждого класса являются минимально необходимыми.
2.1.3. Седьмой класс присваивают СВТ, к которым предъявлялись требования по защите от НСД к информации, но при оценке защищенность

СВТ оказалась ниже уровня требований шестого класса.
2.2. Требования к показателям защищенности шестого класса.
2.2.1. Дискреционный принцип контроля доступа.
КСЗ должен контролировать доступ наименованных субъектов (пользователей) к наименованным объектам (файлам, программам, томам и т. д.).
Для каждой пары (субъект — объект) в СВТ должно быть задано явное и недвусмысленное перечисление допустимых типов доступа (читать, писать и т. д.), т. е. тех типов доступа, которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному ресурсу СВТ (объекту).
КСЗ должен содержать механизм, претворяющий в жизнь дискреционные правила разграничения доступа.
Контроль доступа должен быть применим к каждому объекту и каждому субъекту (индивиду или группе равноправных индивидов).
Механизм, реализующий дискреционный принцип контроля доступа, должен предусматривать возможности санкционированного изменения ПРД, в том числе возможность санкционированного изменения списка пользователей СВТ и списка защищаемых объектов.
Права изменять ПРД должны предоставляться выделенным субъектам (администрации, службе безопасности и т. д.).
2.2.2. Идентификация и аутентификация, КСЗ должен требовать от пользователей идентифицировать себя при запросах на доступ. КСЗ должен подвергать проверке подлинность идентификации — осуществлять аутентификацию. КОЗ должен располагать необходимыми данными для идентификации и аутентификации. КСЗ должен препятствовать доступу к защищаемым ресурсам неидентифицированных пользователей и пользователей, подлинность идентификации которых при аутентификации не подтвердилась.
2.2.3. Тестирование. В СВТ шестого класса должны тестироваться:
>• реализация дискреционных ПРД (перехват явных и скрытых запросов, правильное распознавание санкционированных и несанкционированных запросов на доступ, средства защиты механизма разграничения доступа, санкционированные изменения ПРД);
>• успешное осуществление идентификации и аутентификации, а также их средств защиты.
2.2.4. Руководство для пользователя.
Документация на СВТ должна включать в себя краткое руководство для пользователя с описанием способов использования КСЗ и его интерфейса с пользователем.
2.2.5. Руководство по КСЗ.
Данный документ адресован администратору защиты и должен содержать:
>• описание контролируемых функций;
>• руководство по генерации КСЗ;
5- описание старта СВТ и процедур проверки правильности старта.
2.2.6. Тестовая документация.
Должно быть предоставлено описание тестов и испытаний, которым подвергалось СВТ (в соответствии с п. 2.2.3.) и результатов тестирования.
2.2.7. Конструкторская (проектная) документация.
Должна содержать общее описание принципов работы СВТ, общую схему КСЗ, описание интерфейсов КСЗ с пользователем и интерфейсов частей КСЗ между собой, описание механизмов идентификации и аутентификации.
2.3. Требования к показателям пятого класса защищенности.
2.3.1. Дискреционный принцип контроля доступа.
Данные требования включает в себя аналогичные требование шестого класса (п. 2.2.1).
Дополнительно должны быть предусмотрены средства управления,

ограничивающие распространение прав на доступ.
2.3.2. Очистка памяти.
При первоначальном назначении или при перераспределении внешней памяти КСЗ должен предотвращать доступ субъекту к остаточной информации.
2.3.3. Идентификация и аутентификация. Данные требования полностью совпадают с аналогичными требованиями шестого класса (п. 2.2.2).
2.3.4. Гарантии проектирования.
На начальном этапе проектирования СВТ должна быть построена модель защиты. Модель должна включать в себя ПРД к объектам и непротиворечивые правила изменения ПРД.
2.3.5. Регистрация.
КСЗ должен быть в состоянии осуществлять регистрацию следующих событий:
>• использование идентификационного и аутентификационного механизма;
>• запрос на доступ к Защищаемому ресурсу (открытие файла, запуск программы и т. д.);
>• создание и уничтожение объекта;
>• действия по изменению ПРД.
Для каждого из этих событий должна регистрироваться следующая информация:
>• дата и время;
>• субъект, осуществляющий регистрируемое действие;
>• тип события (если регистрируется запрос на доступ, то следует отмечать объект и тип доступа);
>• успешно ли осуществилось событие (обслужен запрос на доступ или нет).
КСЗ должен содержать средства выборочного ознакомления с регистрационной информацией.
2.3.6. Целостность КСЗ.
В СВТ пятого класса защищенности должны быть предусмотрены средства периодического контроля за целостностью программной и информационной части КСЗ.
2.3.7. Тестирование.
В СВТ пятого класса защищенности должны тестироваться:
>• реализация ПРД (перехват явных и скрытых запросов на доступ, правильное распознавание санкционированных и несанкционированных запросов, средства защиты механизма разграничения доступа, санкционированные изменения ПРД);
>• успешное осуществление идентификации и аутентификации, а также их средства защиты;
>• очистка памяти в соответствии с п. 2.3.2;
>• регистрация событий в соответствии с п. 2.3.5, средства защиты регистрационной информации и возможность санкционированного ознакомления с ней;
>• работа механизма, осуществляющего контроль за целостностью КСЗ.
2.3.8. Руководство пользователя.
Данное требование совпадает с аналогичным требованием шестого класса (п. 2.2.4).
2.3.9. Руководство по КСЗ.
Данный документ адресован администратору защиты и должен содержать:
>• описание контролируемых функций;
>• руководство по генерации КСЗ;
>• описания старта СВТ, процедур проверки правильности старта, процедур работы со средствами регистрации.
2.3.10. Тестовая документация.
Должно быть предоставлено описание тестов и испытаний, которым подвергалось СВТ (в соответствии с требованиями п. 2.3.7), и результатов тестирования.

2.3.11. Конструкторская и проектная документация. Должна содержать:
>• описание принципов работы СВТ;
>• общую схему КСЗ;
>• описание интерфейсов КСЗ с пользователем и интерфейсов модулей КСЗ;
>• модель защиты;
>• описание механизмов контроля целостности КСЗ, очистки памяти, идентификации и аутентификации.
2.4. Требования к показателям четвертого класса защищенности.
2.4.1. Дискреционный принцип контроля доступа.
Данные требования включают аналогичные требования пятого класса (п. 2.3.1).
Дополнительно КСЗ должен содержать механизм, претворяющий в жизнь дискреционные ПРД, как для явных действий пользователя, так и для скрытых, обеспечивая тем самым защиту объектов от НСД (т. е. от доступа, не допустимого с точки зрения заданного ПРД). Под «явными» здесь подразумеваются действия, осуществляемые с использованием системных средств — системных макрокоманд, инструкций языков высокого уровня и т. д., а под «скрытыми» — иные действия, в том числе с использованием собственных программ работы с устройствами.
Дискреционные ПРД для систем данного класса являются дополнением мандатных ПРД.
2.4.2. Мандатный принцип контроля доступа.
Для реализации этого принципа должны сопоставляться классификационные метки каждого субъекта и каждого объекта, отражающие их место в соответствующей иерархии. Посредством этих меток субъектам и объектам должны назначаться классификационные уровни (уровни уязвимости, категории секретности и т. п.), являющиеся комбинациями иерархических и неиерархических категорий. Данные метки должны служить основой мандатного принципа разграничения доступа.
КСЗ при вводе новых данных в систему должен запрашивать и получать от санкционированного пользователя классификационные метки этих данных. При санкционированном занесении в список пользователей нового субъекта должно осуществляться сопоставление ему классификационных меток. Внешние классификационные метки (субъектов, объектов) должны точно соответствовать внутренним меткам (внутри КСЗ).
КСЗ должен реализовывать мандатный принцип контроля доступа применительно ко всем объектам при явном и скрытом доступе со стороны любого из субъектов:
>• субъект может читать объект, только если иерархическая классификация в классификационном уровне субъекта не меньше, чем иерархическая классификация в классификационном уровне объекта, и неиерархические категории в классификационном уровне субъекта включают в себя все иерархические категории в классификационном уровне объекта;
>• субъект осуществляет запись в объект, только если классификационный уровень субъекта в иерархической классификации не больше, чем классификационный уровень объекта в иерархической классификации, и все иерархические категории в классификационном уровне субъекта включаются в неиерархические категории в классификационном уровне объекта.
Реализация мандатных ПРД должна предусматривать возможности сопровождения: изменения классификационных уровней субъектов и объектов специально выделенными субъектами.
В СВТ должен быть реализован диспетчер доступа, т. е. средство, осуществляющее перехват всех обращений субъектов к объектам, а также разграничение доступа в соответствии с заданным принципом разграничения доступа. При этом решение о санкционированности запроса на доступ должно приниматься только при одновременном разрешении его и дискреционными, и мандатными ПРД. Таким образом, должен

контролироваться не только единичный акт доступа, но и потоки информации.

2.4.3. Очистка памяти.

При первоначальном назначении или при перераспределении внешней памяти КСЗ должен затруднять субъекту доступ к остаточной информации. При перераспределении оперативной памяти КСЗ должен осуществлять ее очистку.

2.4.4. Изоляция модулей.

При наличии в СВТ мультипрограммирования в КСЗ должен существовать программно-технический механизм, изолирующий программные модули одного процесса (одного субъекта), от программных модулей других процессов (других субъектов) — т. е. в оперативной памяти ЭВМ программы разных пользователей должны быть защищены друг от друга.

2.4.5. Маркировка документов.

При выводе защищаемой информации на документ в начале и конце проставляют штамп № 1 и заполняют его реквизиты в соответствии с Инструкцией № 0126-87 (п. 577).

2.4.6. Защита ввода и вывода на отчуждаемый физический носитель информации.

КСЗ должен различать каждое устройство ввода-вывода и каждый канал связи как произвольно используемые или идентифицированные («помеченные»). При вводе с «помеченного» устройства (вывода на «помеченное» устройство) КСЗ должен обеспечивать соответствие между меткой вводимого (выводимого) объекта (классификационным уровнем) и меткой устройства. Такое же соответствие должно обеспечиваться при работе с «помеченным» каналом связи.

Изменения в назначении и разметке устройств и каналов должны осуществляться только под контролем КСЗ.

2.4.7. Сопоставление пользователя с устройством.

КСЗ должен обеспечивать вывод информации на запрошенное пользователем устройство как для произвольно используемых устройств, так и для идентифицированных (при совпадении маркировки).

Идентифицированный КСЗ должен включать в себя механизм, посредством которого санкционированный пользователь надежно сопоставляется выделенному устройству.

2.4.8. Идентификация и аутентификация.

КСЗ должен требовать от пользователей идентифицировать, себя при запросах на доступ, должен проверять подлинность идентификатора субъекта — осуществлять аутентификацию. КСЗ должен располагать необходимыми данными для идентификации и аутентификации и препятствовать входу в СВТ неидентифицированного пользователя или пользователя, чья подлинность при аутентификации не подтвердилась.

КСЗ должен обладать способностью надежно связывать полученную идентификацию со всеми действиями данного пользователя.

2.4.9. Гарантии проектирования.

Проектирование КСЗ должно начинаться с построения модели защиты, содержащей:

>• непротиворечивые ПРД;

**>•** непротиворечивые правила изменения ПРД;

>• правила работы с устройствами ввода и вывода информации и каналами связи.

2.4.10. Регистрация.

Данные требования включают аналогичные требования пятого класса защищенности (п. 2.3.5). Дополнительно должна быть предусмотрена регистрация всех попыток доступа, всех действий оператора и выделенных пользователей (администраторов защиты и т. п.).

2.4.11. Целостность КСЗ.

В СВТ четвертого класса защищенности должен осуществляться периодический контроль за целостностью КСЗ.
Программы КСЗ должны выполняться в отдельной части оперативной памяти.
2.4.12. Тестирование.
В четвертом классе защищенности должны тестироваться:
>• реализация ПРД (перехват запросов на доступ, правильное распознавание санкционированных и несанкционированных запросов в соответствии с дискреционными и мандатными правилами, верное сопоставление меток субъектов и объектов, запрос меток вновь вводимой информации, средства защиты механизма разграничения доступа, санкционированное изменение ПРД);
>• невозможность присвоения субъектом себе новых прав;
>• очистка оперативной и внешней памяти;
>• работа механизма изоляции процессов в оперативной памяти;
>• маркировка документов;
>• защита вода и вывода информации на отчуждаемый физический носитель и сопоставление пользователя с устройством;
>• идентификация и аутентификация, а также их средства защиты;
>• запрет на доступ несанкционированного пользователя;
>• работа механизма, осуществляющего контроль за целостностью СВТ;
>• регистрация событий, описанных в п. 2.4.10, средства защиты регистрационной информации и возможность санкционированного ознакомления с этой информацией.
2.4.13. Руководство для пользователя.
Данное требование совпадает с аналогичным требованием шестого (п. 2.2.4) и пятого (п. 2.3.8) классов.
2.4.14. Руководство по КСЗ.
Данные требования полностью совпадают с аналогичными требованиями пятого класса (п. 2.3.9).
2.4.15. Тестовая документация.
Должно быть представлено описание тестов и испытаний, которым подвергалось СВТ (в соответствии с п. 2.4.12) и результатов тестирования.
2.4.16. Конструкторская (проектная) документация.
Должна содержать:
>• общее описание принципов работы СВТ;
>• общую схему КСЗ;
>• описание внешних интерфейсов КСЗ и интерфейсов модулей КСЗ;
>• описание модели защиты;
>• описание диспетчера доступа;
>• описание механизма контроля целостности КСЗ;
>• описание механизма очистки памяти;
>• описание механизма изоляции программ в оперативной памяти;
>• описание средств защиты ввода и вывода на отчуждаемый физический носитель информации и сопоставления пользователя с устройством;
>• описание механизма идентификации и аутентификации;
>• описание средств регистрации.
2.5. Требования к показателям третьего класса защищенности.
2.5.1. Дискреционный принцип контроля доступа. Данные требования полностью совпадают с требованиями пятого (п. 2.3.1) и четвертого классов (п. 2.4.1) классов.
2.5.2. Мандатный принцип контроля доступа. Данные требования полностью совпадают с аналогичным требованием четвертого класса (п. 2.4.2).
2.5.3. Очистка памяти.
Для СВТ третьего класса защищенности КСЗ должен осуществлять очистку оперативной и внешней памяти. Очистка должна производиться путем записи маскирующей информации в память при ее освобождении

(перераспределении).
2.5.4. Изоляция модулей.
Данные требования полностью совпадают с аналогичным требованием четвертого класса (п. 2.4.4).
2.5.5. Маркировка документов.
Данные требования полностью совпадают с аналогичным требованием четвертого класса (п. 2.4.5).
2.5.6. Защита ввода и вывода на отчуждаемый физический носитель информации.
Данные требования полностью совпадают с аналогичным требованием четвертого класса (п. 2.4.6).
2.5.7. Сопоставление пользователя с устройством. Данные требования полностью совпадают с аналогичным требованием четвертого класса (п. 2.4.7).
2.5.8. Идентификация и аутентификация. Данные требования полностью совпадают с аналогичным требованием четвертого класса (п. 2.4.8).
2.5.9. Гарантии проектирования.
На начальном этапе проектирования КСЗ должна строиться модель защиты, задающая принцип разграничения доступа и механизм управления доступом. Эта модель должна содержать:
>• непротиворечивые правила изменения ПРД;
>• правила работы с устройствами ввода и вывода;
>• формальную модель механизма управления доступом. Должна предлагаться высокоуровневая спецификация части КСЗ, реализующего механизм управления доступом и его интерфейсов. Эта спецификация должна быть верифицирована на соответствие заданных принципов разграничения доступа.
2.5.10. Регистрация.
Данные требования полностью совпадают с аналогичным требованием четвертого класса (п. 2.4.10).
2.5.11. Взаимодействие пользователя с КСЗ.
Для обеспечения возможности изучения, анализа, верификации и модификации КСЗ должен быть хорошо структурирован, его структура должна быть модульной и четко определенной. Интерфейс пользователя и КСЗ должен быть определен (вход в систему, запросы пользователей и КСЗ и т. п.). Должна быть обеспечена надежность такого интерфейса. Каждый интерфейс пользователя и КСЗ должен быть логически изолирован от других таких же интерфейсов.
2.5.12. Надежное восстановление
Процедуры восстановления после сбоев и отказов оборудования должны обеспечивать полное восстановление свойств КСЗ.
2.5.13. Целостность КСЗ.
Необходимо осуществлять периодический контроль за целостностью КСЗ. Программы должны выполняться в отдельной части оперативной памяти. Это требование должно подвергаться верификации.
2.5.14. Тестирование.
СВТ должны подвергаться такому же тестированию, что и СВТ четвертого класса (п. 2.4.12).
Дополнительно должны тестироваться:
>• очистка памяти (п. 2.5.3);
**>•** работа механизма надежного восстановления.
2.5.15. Руководство для пользователя.
Данные требования полностью совпадают с аналогичным требованием четвертого класса (п. 2.4.13).
2.5.16. Руководство по КСЗ.
Документ адресован администратору защиты и должен содержать:
>• описание контролируемых функций;

>• руководство по генерации КСЗ;
>• описание старта СВТ, процедур проверки правильности старта, процедур работы со средствами регистрации;
>• руководство по средствам надежного восстановления.
2.5.17. Тестовая документация
В документации должно быть представлено описание тестов и испытаний, которым подвергалось СВТ (п. 2.5.14), а также результатов тестирования.
2.5.18. Конструкторская (проектная) документация.
Требуется такая же документация, что и для СВТ четвертого класса (п. 2.4.16). Дополнительно необходимы:
>• высокоуровневая спецификация КСЗ и его интерфейсов;
>• верификация соответствия высокоуровневой спецификации КСЗ модели защиты,
2.6. Требования к показателям второго класса защищенности.
2.6.1. Дискреционный принцип контроля доступа.
Данные требования включают аналогичные требования третьего класса (п. 2.5.1).
Дополнительно требуется, чтобы дискреционные правила разграничения доступа были эквивалентны мандатным правилам (т. е. всякий запрос на доступ должен быть одновременно санкционированным или несанкционированным одновременно и по дискреционным правилам, и по мандатным ПРД).
2.6.2. Мандатный принцип контроля доступа. Данные требования полностью совпадают с аналогичным требованием третьего класса (п. 2.5.2).
2.6.3. Очистка памяти.
Данные требования полностью совпадают с аналогичным требованием третьего класса (п. 2.5.3).
2.6.4. Изоляция модулей.
При наличии в СВТ мультипрограммирования в КСЗ должен существовать программно-технический механизм, изолирующий программные модули одного процесса (одного субъекта), от программных модулей других процессов (других субъектов) — т. е. в оперативной памяти ЭВМ программы разных пользователей должны быть изолированы друг от друга. Гарантии изоляции должны быть основаны на архитектуре СВТ.
2.6.5. Маркировка документов.
Данные требования полностью совпадают с аналогичным требованием четвертого класса (п. 2.5.5). -
2.6.6. Защита ввода и вывода на отчуждаемый физический носитель информации.
Данные требования полностью совпадают с аналогичным требованием третьего класса (п. 2.5.6).
2.6.7. Сопоставление пользователя с устройством. Данные требования полностью совпадают с аналогичным требованием четвертого (п. 2.4.7) и. третьего (п. 2.5.7) классов.
2.6.8. Идентификация и аутентификация. Требование полностью совпадает с аналогичным требованием четвертого (п. 2.4.8) и третьего (п. 2.5.8) классов.
2.6.9. Гарантии проектирования.
Данные требования включают аналогичные требования третьего класса (п. 2.5.9).
Дополнительно требуется, чтобы высокоуровневые спецификации КСЗ были отображены последовательно в спецификации одного или нескольких нижних уровней, вплоть до реализации высокоуровневой спецификации КСЗ на языке программирования высокого уровня. При этом методами верификации должно осуществляться доказательство соответствия каждого такого отображения спецификациям высокого (верхнего для данного отображения) уровня. Этот процесс может включать в себя как одно отображение (высокоуровневая

спецификация — язык программирования), так и последовательность отображений в промежуточные спецификации с понижением уровня, вплоть до языка программирования. В результате верификации соответствия каждого уровня предыдущему должно достигаться соответствие реализации высокоуровневой спецификации КСЗ модели защиты, изображенной на чертеже (см. рис. Схема модели защиты).

2.6.10. Регистрация.

Данные требования полностью совпадают с аналогичным требованием четвертого (п. 2.4.10) и третьего (п. 2.5.10) классов.

2.6.11. Взаимодействие пользователя с КСЗ. Данные требования полностью совпадают с аналогичным требованием третьего класса (п. 2.5.11).

2.6.12. Надежное восстановление.

Данные требования полностью совпадают с аналогичным требованием третьего класса (п. 2.5.12).

2.6.13. Целостность КСЗ.

Данные требования полностью совпадают с аналогичным требованием третьего класса (п. 2.5.13).

2.6.14. Контроль модификации.

При проектировании, построении и сопровождении СВТ должно быть предусмотрено управление конфигурацией СВТ, т. е. контроль изменений в формальной модели, спецификациях (разных уровней), документации, исходном тексте, версии в объектном коде. Должно обеспечиваться соответствие между документацией и текстами программ. Должна осуществляться сравниваемость генерируемых версий. Оригиналы программ должны быть защищены.

2.6.15. Контроль дистрибуции.

Должен осуществляться контроль точности копирования в СВТ при изготовлении копий с образца. Изготовляемая копия должна гарантированно повторять образец.

2.6.16. Тестирование.

СВТ второго класса должны тестироваться так же, как и СВТ третьего класса (п. 2.5.14).

Дополнительно должен тестироваться контроль дистрибуции.

2.6.17. Руководство для пользователя.

Данные требования полностью совпадают с аналогичным требованием четвертого (п. 2.4.13) и третьего (п. 2.5.15) классов.

2.6.18. Руководство по КСЗ.

Данные требования включают аналогичные требования третьего класса (п. 2.5.16).

Дополнительно должны быть представлены руководства по надежному восстановлению, по работе со средствами контроля модификации и дистрибуции.

2.6.19. Тестовая документация.

Должно быть представлено описание тестов и испытаний, которым подвергалось СВТ (п. 2.6.16), а также результатов тестирования.

2.6.20. Конструкторская (проектная) документация.

Требуется такая же документация, что и для СВТ третьего класса (п. 2.5.18).

Дополнительно должны быть описаны гарантии процесса проектирования и эквивалентность дискреционных (п. 2.6.1) и мандатных (п. 2.6.2) ПРД.

2.7. Требования к показателям первого класса защищенности.

2.7.1. Дискреционный принцип контроля доступа. Данные требования полностью совпадают с аналогичным требованием второго класса (п. 2.6.1).

2.7.2. Мандатный принцип контроля доступа. Данные требования полностью совпадают с аналогичным требованием второго класса (п. 2.6.2).

2.7.3. Очистка памяти.

Данные требования полностью совпадают с аналогичным требованием второго класса (п. 2.6.3).
2.7.4. Изоляция модулей.
Данные требования полностью совпадают с аналогичным требованием второго класса (п. 2.6.4).
2.7.5. Маркировка документов.
Данные требования полностью совпадают с аналогичным требованием второго класса (п. 2.6.5).
2.7.6. Защита ввода и вывода на отчуждаемый физический носитель информации.
Данные требования полностью совпадают с аналогичным требованием второго класса (п. 2.6.6).
2.7.7. Сопоставление пользователя с устройством. Данные требования полностью совпадают с аналогичным требованием второго класса (п. 2.6.7).
2.7.8. Идентификация и аутентификация. Данные требования полностью совпадают с аналогичным требованием второго класса (п. 2.6.8).
2.7.9. Гарантии проектирования.
Данные требования включают с аналогичные требования второго класса (п. 2.6.9).
Дополнительно требуется верификация соответствия объектного кода тексту КСЗ на языке высокого уровня.
2.7.10. Регистрация.
Данные требования полностью совпадают с аналогичным требованием второго класса (п. 2.6.10).
2.7.11. Взаимодействие пользователя с КСЗ. Данные требования полностью совпадают с аналогичным требованием второго класса (п. 2.6.11).
2.7.12. Надежное восстановление.
Данные требования полностью совпадают с аналогичным требованием второго класса (п. 2.6.12).
2.7.13. Целостность КСЗ.
Данные требования полностью совпадают с аналогичным требованием второго класса (п. 2.6.13).
2.7.14. Контроль модификации.
Данные требования полностью совпадают с аналогичным требованием второго класса (п. 2.6.14).
2.7.15. Контроль дистрибуции.
Данные требования полностью совпадают с аналогичным требованием второго класса (п. 2.6.15).
2.7.16. Гарантии архитектуры.
КСЗ должен обладать механизмом, гарантирующим перехват диспетчером доступа всех обращений субъектов к объектам.
2.7.17: Тестирование.
Данные требования полностью совпадают с аналогичным требованием второго класса (п. 2.6.16).
2.7.18. Руководство пользователя.
Данные требования полностью совпадают с аналогичным требованием второго класса (п:2.6.17).
2.7.19. Руководство по КСЗ
Данные требования полностью совпадают с аналогичным требованием второго класса (п. 2.6.18).
2.7.20. Тестовая документация
Данные требования полностью совпадают с аналогичным требованиями второго класса (п. 2.6.19).
2.7.21. Конструкторская (проектная) документация
Требуется такая же документация, что и для СВТ второго класса (п. 2.6.20).

Дополнительно разрабатывается описание гарантий процесса проектирования (п. 2.7.9).

**3. Оценка класса защищенности СВТ (сертификация СВТ)**

Оценка класса защищенности СВТ проводится в соответствии с Положением о сертификации средств и систем вычислительной техники и связи по требованиям защиты информации, Временным положением по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники и другими документами.

**«СРЕДСТВА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ. МЕЖСЕТЕВЫЕ ЭКРАНЫ. ЗАЩИТА ОТ НСД К ИНФОРМАЦИИ. ПОКАЗАТЕЛИ ЗАЩИЩЕННОСТИ ОТ НСД К ИНФОРМАЦИИ» Руководящий документ Гостехкомиссии РФ**

Настоящий руководящий документ устанавливает классификацию межсетевых экранов (МЭ) по уровню защищенности от несанкционированного доступа (НСД) к информации на базе перечня показателей защищенности и совокупности описывающих их требований.

Под сетями ЭВМ, распределенными автоматизированными системами (АС) в данном документе понимаются соединенные каналами связи системы обработки данных, ориентированные на конкретного пользователя.

МЭ представляет собой локальное (однокомпонентное) или функционально-распределенное средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС, и обеспечивает защиту АС посредством фильтрации информации, т. е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС.

Руководящий документ разработан в дополнение к Руководящим документам Гостехкомиссии России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» и «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

Документ предназначен для заказчиков и разработчиков МЭ, а также сетей ЭВМ, распределенных автоматизированных систем с целью использования при формулировании и реализации требований по их защите от НСД к информации.

**1. Общие положения**

1.1. Данные показатели содержат требования к средствам защиты, обеспечивающим безопасное взаимодействие сетей ЭВМ, АС посредством управления межсетевыми потоками информации, и реализованных в виде МЭ.

1.2. Показатели защищенности применяются к МЭ для определения уровня защищенности, который они обеспечивают при межсетевом взаимодействии. Конкретные перечни показателей определяют классы защищенности МЭ.

1.3. Деление МЭ на соответствующие классы по уровням контроля межсетевых информационных потоков с точки зрения защиты информации необходимо в целях разработки и применения обоснованных и экономически оправданных мер по достижению требуемого уровня защиты информации при взаимодействии сетей ЭВМ, АС.

1.4. Дифференциация подхода к выбору функций защиты в МЭ определяется АС, для защиты которой применяется данный экран.

1.5. Устанавливается пять классов защищенности МЭ.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите информации.

Самый низкий класс защищенности — пятый, применяемый для безопасного взаимодействия АС класса 1Д с внешней средой, четвертый — для 1Г, третий — 1В, второй — 1Б, самый высокий — первый, применяемый для

безопасного взаимодействия АС класса 1А с внешней средой.
1.6. Требования, предъявляемые к МЭ, не исключают требований, предъявляемых к средствам вычислительной техники (СВТ) и АС в соответствии с руководящими документами Гостехкомиссии России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» и «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».
При включении МЭ в АС определенного класса защищенности, класс защищенности совокупной АС, полученной из исходной путем добавления в нее МЭ, не должен понижаться.
Для АС класса 3Б, 2Б должны применяться МЭ не ниже 5-го класса.
Для АС класса 3А, 2А в зависимости от важности обрабатываемой информации должны применяться МЭ следующих классов:
>• при обработке информации с грифом «секретно» — не ниже 3-го класса;
>• при обработке информации с грифом «совершенно секретно» — не ниже 2-го класса;
>• при обработке информации с грифом «особой важности» — не ниже 1-го класса.

**2. Требования к межсетевым экранам**

2.1. Показатели защищенности
2.1.1. Перечень показателей по классам защищенности МЭ.
Показатель защищенности /Класс защищенности
/5 /4 /3 /2 /1
Управление доступом (фильтрация данных и трансляция адресов) /+ /+ /+ /+ /=
Идентификация и аутентификация /— /— /+ /= /+
Регистрация /— /+ /+ /+ /=
Администрирование: идентификация и аутентификация /+ /= /+ /+ /+
Администрирование: регистрация /+ /+ /+ /= /=
Администрирование: простота использования /— /— /+ /= /+
Целостность /+ /= /+ /+ /+
Восстановление /+ /= /= /+ /=
Тестирование /+ /+ /+ /+ /- +
Руководство администратора защиты /+ /= /= /= /=
Тестовая документация /+ /+ /+ /+ /+
Конструкторская (проектная) документация /+ /= /+ /= /+
Обозначения:
«-» — нет требований к данному классу;
«+» — новые или дополнительные требования;
«=» — требования совпадают с требованиями к МЭ предыдущего класса.
2.2. Требования к пятому классу защищенности МЭ.
2.2.1. Управление доступом.
МЭ должен обеспечивать фильтрацию на сетевом уровне. Решение по фильтрации может приниматься для каждого сетевого пакета независимо на основе, по крайней мере, сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов.
2.2.2. Администрирование: идентификация и аутентификация. МЭ должен обеспечивать идентификацию и аутентификацию администратора МЭ при его локальных запросах на доступ. МЭ должен предоставлять возможность для идентификации и аутентификации по идентификатору (коду) и паролю условно-постоянного действия.
2.2.3. Администрирование: регистрация.
МЭ должен обеспечивать регистрацию входа (выхода) администратора МЭ в систему (из системы) либо загрузки и инициализации системы и ее

программного останова. Регистрация выхода из системы не проводится в моменты аппаратурного отключения МЭ.
В параметрах регистрации указываются:
>• дата, время и код регистрируемого события;
>• результат попытки осуществления регистрируемого события — успешная или неуспешная;
>• идентификатор администратора МЭ, предъявленный при попытке осуществления регистрируемого события.
2.2.4. Целостность.
МЭ должен содержать средства контроля за целостностью своей программной и информационной части.
2.2.5. Восстановление.
МЭ должен предусматривать процедуру восстановления после сбоев и отказов оборудования, которые должны обеспечивать восстановление свойств МЭ.
2.2.6. Тестирование.
В МЭ должна обеспечиваться возможность регламентного тестирования:
>• реализации правил фильтрации (см. п. 2.2.1);
>• процесса идентификации и аутентификации администратора МЭ (см. п. 2.2.2);
>• процесса регистрации действий администратора МЭ (см. п. 2.2.3.);
>• процесса контроля за целостностью программной и информационной части МЭ (см. п. 2.2.4);
>• процедуры восстановления (см. п. 2.2.5.).
2.2.7. Руководство администратора МЭ. Документ содержит:
>• описание контролируемых функций МЭ;
>• руководство по настройке и конфигурированию МЭ;
>• описание старта МЭ и процедур проверки правильности старта;
>• руководство по процедуре восстановления.
2.2.8. Тестовая документация.
Должна содержать описание тестов и испытаний, которым подвергался МЭ (в соответствии с п. 2.2.6), и результаты тестирования.
2.2.9. Конструкторская (проектная) документация. Должна содержать:
>• общую схему МЭ;
>• общее описание принципов работы МЭ;
>• описание правил фильтрации;
>• описание средств и процесса идентификации и аутентификации;
>• описание средств и процесса регистрации;
>• описание средств и процесса контроля за целостностью программной и информационной части МЭ;
>• описание процедуры восстановления свойств МЭ. 2.3. Требования к четвертому классу защищенности МЭ.
2.3.1. Управление доступом.
Данные требования полностью включают аналогичные требования пятого класса (п. 2.2.1).
Дополнительно МЭ должен обеспечивать:
>• фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
>• фильтрацию с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;
>• фильтрацию с учетом любых значимых полей сетевых пакетов.
2.3.2. Регистрация.
МЭ должен обеспечивать возможность регистрации и учета фильтруемых пакетов. В параметры регистрации включаются адрес, время и результат фильтрации.
2.3.3. Администрирование: идентификация и аутентификация. Данные требования полностью совпадают с аналогичными требованиями пятого

класса (п. 2.2.2).
2.3.4. Администрирование: регистрация. Данные требования включают аналогичные требования пятого класса (п. 2.2.3). Дополнительно МЭ должен обеспечивать регистрацию запуска программ и процессов (заданий, задач).
2.3.5. Целостность.
Данные требования полностью совпадают с аналогичными требованиями пятого класса (п. 2.2.4).
2.3.6. Восстановление.
Данные требования полностью совпадают с аналогичными требованиями пятого класса (п. 2.2.5).
2.3.7. Тестирование.
В МЭ должна обеспечиваться возможность регламентного тестирования:
>• реализации правил фильтрации (см. п. 2.3.1);
>• процесса регистрации (см. п. 2.3.2);
>• процесса идентификации и аутентификации администратора МЭ (см. п. 2.3.3);
>• процесса регистрации действий администратора МЭ (см. п. 2.3.4);
>• процесса контроля за целостностью программной и информационной части МЭ (см. п. 2.3.5);
>• процедуры восстановления (см. п. 2.3.6).
2.3.8. Руководство администратора МЭ. Данные требования полностью совпадают с аналогичными требованиями пятого класса (п. 2.2.7).
2.3.9. Тестовая документация.
Должна содержать описание тестов и испытаний, которым подвергался МЭ (в соответствии с п. 2.3.7), и результаты тестирования.
2.3.10. Конструкторская (проектная) документация.
Данные требования полностью совпадают с аналогичным» требованиями пятого класса (п. 2.2.9) по составу документации.
2.4. Требования к третьему классу защищенности МЭ.
2.4.1. Управление доступом.
Данные требования полностью включают аналогичные требования четвертого класса (п. 2.3.1).
Дополнительно МЭ должен обеспечивать:
**>•** фильтрацию на транспортном уровне запросов на установление виртуальных соединений. При этом, по крайней мере, учитываются транспортные адреса отправителя и получателя;
>• фильтрацию на прикладном уровне запросов к прикладным сервисам. При этом, по крайней мере, учитываются прикладные адреса отправителя и получателя; фильтрацию с учетом даты/времени.
2.4.2. Идентификация и аутентификация.
МЭ должен обеспечивать возможность аутентификации входящих и исходящих запросов методами, устойчивыми к пассивному и/или активному прослушиванию сети.
2.4.3. Регистрация.
Данные требования включают аналогичные требования четвертого класса (п.2.3.2).
Дополнительно МЭ должен обеспечивать:
**>•** регистрацию и учет запросов на установление виртуальных соединений;
>• локальную сигнализацию попыток нарушения правил фильтрации.
2.4.4. Администрирование: идентификация и аутентификация. Данные требования включают аналогичные требования пятого класса (п.2.2.2). Дополнительно МЭ должен препятствовать доступу неидентифицированного субъекта или субъекта, подлинность идентификации которого при аутентификации не подтвердилась.
При удаленных запросах администратора МЭ на доступ идентификация и аутентификация должны обеспечиваться методами, устойчивыми к пассивному

и активному перехвату информации.
2.4.5. Администрирование: регистрация.
Данные требования полностью включают аналогичные требования четвертого класса (п. 2.3.4).
Дополнительно МЭ должен обеспечивать регистрацию действия администратора МЭ по изменению правил фильтрации.
2.4.6. Администрирование: простота использования.
Многокомпонентный МЭ должен обеспечивать возможность дистанционного управления своими компонентами, в том числе, возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации.
2.4.7. Целостность.
Данные требования полностью включают аналогичные требования пятого класса (п. 2.2.4).
Дополнительно должен обеспечиваться контроль целостности программной и информационной части МЭ по контрольным суммам.
2.4.8. Восстановление.
Данные требования полностью совпадают с аналогичными требованиями пятого класса (п. 2.2.5).
2.4.9. Тестирование.
В МЭ должна обеспечиваться возможность регламентного тестирования:
>• реализации правил фильтрации (см. п. 2.4.1);
>• процесса регистрации (см. п. 2.4.3);
>• процесса идентификации и аутентификации запросов (см. п. 2.4.2);
>• процесса идентификации и аутентификации администратора МЭ (см. п. 2.4.4);
>• процесса регистрации действий администратора МЭ (см. п. 2.4.5);
>• процесса контроля за целостностью программной и информационной части МЭ (см. п. 2.4.7);
>• процедуры восстановления (см. п. 2.4.8.).
2.4.10. Руководство администратора МЭ. Данные требования полностью совпадают **с** аналогичными требованиями пятого класса (п. 2.2.7).
2.4.11. Тестовая документация.
Должна содержать описание тестов и испытаний, которым подвергался МЭ (в соответствии с п. 2.4.9), и результаты тестирования.
2.4.12. Конструкторская (проектная) документация.
Данные требования полностью включают аналогичные требования пятого класса (п. 2.2.9) по составу документации.
Дополнительно документация должна содержать описание средств и процесса централизованного управления компонентами МЭ.
2.5. Требования ко второму классу защищенности МЭ.
2.5.1. Управление доступом.
Данные требования включают аналогичные требования третьего класса (п. 2.4.1).
Дополнительно МЭ должен обеспечивать:
**>•** возможность сокрытия субъектов (объектов) и/или прикладных функций защищаемой сети;
>• возможность трансляции сетевых адресов.
2.5.2. Идентификация и аутентификация. Данные требования полностью совпадают с аналогичными требованиями третьего класса (п. 2.4.2).
2.5.3. Регистрация.
Данные требования включают аналогичные требования третьего класса (п. 2.4.3).
Дополнительно МЭ должен обеспечивать:
>• дистанционную сигнализацию попыток нарушения правил фильтрации;
>• регистрацию и учет запрашиваемых сервисов прикладного уровня;
>• программируемую реакцию на события в МЭ.

2.5.4. Администрирование: идентификация и аутентификация. МЭ должен обеспечивать идентификацию и аутентификацию администратора МЭ при его запросах на доступ. МЭ должен предоставлять возможность для идентификации и аутентификации по идентификатору (коду) и паролю временного действия. МЭ должен препятствовать доступу неидентифицированного субъекта или субъекта, подлинность идентификации которого при аутентификации не подтвердилась.
При удаленных запросах на доступ администратора МЭ идентификация и аутентификация должны обеспечиваться методами, устойчивыми к пассивному и активному перехвату информации.
2.5.5. Администрирование: регистрация. Данные требования полностью совпадают с аналогичными требованиями третьего класса (п. 2.4.5).
2.5.6. Администрирование: простота использования. Данные требования полностью совпадают с аналогичными требованиями третьего класса (п. 2.4.6).
2.5.7. Целостность.
МЭ должен содержать средства контроля за целостностью своей программной и информационной части по контрольным суммам как в процессе загрузки, так и динамически.
2.5.8. Восстановление.
МЭ должен предусматривать процедуру восстановления после сбоев и отказов оборудования, которые должны обеспечивать оперативное восстановление свойств МЭ.
2.5.9. Тестирование.
В МЭ должна обеспечиваться возможность регламентного тестирования:
>• реализации правил фильтрации (см. п. 2.5.1);
>• процесса идентификации и аутентификации (см. п. 2.5.2);
>• процесса регистрации (см. п. 2.5.3);
>• процесса идентификации и аутентификации администратора МЭ (см. п. 2.5.4);
>• процесса регистрации действий администратора МЭ (см. п. 2.5.5);
>• процесса контроля за целостностью программной и информационной части МЭ (см. п. 2.5.7);
>• процедуры восстановления (см. п. 2.5.8).
2.5.10. Руководство администратора МЭ. Данные требования полностью совпадают с аналогичными требованиями пятого класса (п. 2.2.7).
2.5.11. Тестовая документация.
Должна содержать описание тестов и испытаний, которым подвергался МЭ (в соответствии с п. 2.5.9), и результаты тестирования.
2.5.12. Конструкторская (проектная) документация. Данные требования полностью совпадают с аналогичными требованиями третьего класса (п. 2.4.12) по составу документации. 2.6. Требования к первому классу защищенности МЭ.
2.6.1. Управление доступом.
Данные требования полностью совпадают с аналогичными требованиями второго класса (п. 2.5.1).
2.6.2. Идентификация и аутентификация.
Данные требования полностью включают аналогичные требования второго класса (п. 2.5.2).
Дополнительно МЭ должен обеспечивать идентификацию и аутентификацию всех субъектов прикладного уровня.
2.6.3. Регистрация.
Данные требования полностью совпадают с аналогичными требованиями второго класса (п. 2.5.3).
2.6.4. Администрирование: идентификация и аутентификация. МЭ должен обеспечивать идентификацию и аутентификацию администратора МЭ при его запросах на доступ. МЭ должен предоставлять возможность для

идентификации и аутентификации по биометрическим характеристикам или специальным устройствам (жетонам, картам, электронным ключам) и паролю временного действия. МЭ должен препятствовать доступу неидентифицированного субъекта или субъекта, подлинность идентификации которого при аутентификации не подтвердилась.
При удаленных запросах на доступ администратора МЭ идентификация и аутентификация должны обеспечиваться методами, устойчивыми к пассивному и активному перехвату информации.
2.6.5. Администрирование: регистрация. Данные требования полностью совпадают с аналогичными требованиями третьего класса (п. 2.4.5).
2.6.6. Администрирование: простота использования.
Многокомпонентный МЭ должен обеспечивать возможность централизованного управления своими компонентами, в том числе, конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации.
Должен быть предусмотрен графический интерфейс для управления МЭ.
2.6.7. Целостность.
МЭ должен содержать средства контроля за целостностью своей программной и информационной части по контрольным суммам аттестованного алгоритма как в процессе загрузки, так и динамически.
2.6.8. Восстановление.
Данные требования полностью совпадают с аналогичными требованиями второго класса (п. 2.5.8).
2.6.9. Тестирование.
В МЭ должна обеспечиваться возможность регламентного тестирования:
>• реализации правил фильтрации (см. п. 2.6.1);
>• процесса идентификации и аутентификации (см. п. 2.6.2);
>• процесса регистрации (см. п. 2.6.3);
>• процесса идентификации и аутентификации администратора МЭ (см. п. 2.6.4);
>• процесса регистрации действий администратора МЭ (см. п. 2.6.5);
>• процесса централизованного управления компонентами МЭ и графический интерфейс для управления МЭ (см. п. 2.6.6);
>• процесса контроля за целостностью программной и информационной части МЭ (см. п. 2.6.7);
>• процедуры восстановления (см. п. 2.6.8).
2.6.10. Руководство администратора МЭ. Данные требования полностью совпадают с аналогичными требованиями пятого класса (п.2.2.7).
2.6.11. Тестовая документация.
Должна содержать описание тестов и испытаний, которым подвергался МЭ (в соответствии с п. 2.6.9), и результаты тестирования.
2.6.12. Конструкторская (проектная) документация. Данные требования полностью включают аналогичные требования третьего класса (п. 2.4.12) по составу документации.
Дополнительно документация должна содержать описание графического интерфейса для управления МЭ.

**3. Термины и определения**

Администратор МЭ — лицо, ответственное за сопровождение МЭ.
Дистанционное управление компонентами МЭ — выполнение функций по сопровождению МЭ (компоненты) администратором МЭ с узла (рабочей станции) сети, на котором не функционирует МЭ (компонента) с использованием сетевых протоколов.
Критерии фильтрации — параметры, атрибуты, характеристики, на основе которых осуществляется разрешение или запрещение дальнейшей передачи пакета (данных) в соответствии с заданными правилами разграничения доступа (правилами фильтрации). В качестве таких параметров могут использоваться служебные поля пакетов (данных), содержащие сетевые

адреса, идентификаторы, адреса интерфейсов, портов и другие значимые данные, а также внешние характеристики, например, временные, частотные характеристики, объем данных и т. п.

Локальное (местное) управление компонентами МЭ — выполнение функций по сопровождению МЭ (компоненты) администратором МЭ на том же узле (платформе), на котором функционирует МЭ (компонента) с использованием интерфейса МЭ.

Межсетевой экран (МЭ) — это локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС. МЭ обеспечивает защиту АС посредством фильтрации информации, т. е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС на основе заданных правил, проводя таким образом разграничение доступа субъектов из одной АС к объектам другой АС. Каждое правило запрещает или разрешает передачу информации определенного вида между субъектами и объектами. Как следствие, субъекты из одной АС получают доступ только к разрешенным информационным объектам из другой АС. Интерпретация набора правил выполняется последовательностью фильтров, которые разрешают или запрещают передачу данных (пакетов) на следующий фильтр или уровень протокола.

Правила фильтрации — перечень условий по которым с использованием заданных критериев фильтрации осуществляется разрешение или запрещение дальнейшей передачи пакетов (данных) и перечень действий, производимых МЭ по регистрации и/или осуществлению дополнительных защитных функций.

Межсетевой экран может строиться с помощью экранирующих агентов, которые обеспечивают установление соединения между субъектом и объектом, а затем пересылают информацию, осуществляя контроль и/или регистрацию. Использование экранирующих агентов позволяет предоставить дополнительную защитную функцию — сокрытие от субъекта истинного объекта. В то же время, субъекту кажется, что он непосредственно взаимодействует с объектом. Обычно экран не является симметричным, для него определены понятия «внутри» и «снаружи». При этом задача экранирования формулируется как защита внутренней области от неконтролируемой и потенциально враждебной внешней.

Сетевые адреса —адресные данные, идентифицирующие субъекты и объекты и используемые протоколом сетевого уровня модели международной организации по стандартизации взаимодействия открытых систем (ISO OSI). Сетевой протокол выполняет управление коммуникационными ресурсами, маршрутизацию пакетов, их компоновку для передачи в сети. В этих протоколах решается возможность доступа к подсети, определяется маршрут передачи и осуществляется трансляция сообщения. Управление доступом на сетевом уровне позволяет отклонять нежелательные вызовы и дает возможность различным подсетям управлять использованием ресурсов сетевого уровня. Поэтому в данных протоколах возможно выполнение требований по защите в части проверки подлинности сетевых ресурсов, источника и приемника данных, принимаемых сообщений, проведения контроля доступа к ресурсам сети.

Трансляция адреса — функция МЭ, скрывающая внутренние адреса объектов (субъектов) от внешних субъектов.

Транспортные адреса — адресные данные, идентифицирующие субъекты и объекты и используемые протоколом транспортного уровня модели ISO OSI. Протоколы транспортного уровня обеспечивают создание и функционирование логических каналов между программами (процессами, пользователями) в различных узлах сети, управляют потоками информации между портами, осуществляют компоновку пакетов о запросах и ответах.

Централизованное управление компонентами МЭ — выполнение с одного

рабочего места (рабочей станции, узла) всех функций по сопровождению МЭ (его компонент), только со стороны санкционированного администратора, включая инициализацию, останов, восстановление, тестирование, установку и модификацию правил фильтрации данных, параметров регистрации, дополнительных защитных функций и анализ зарегистрированных событий.

Экранирование — функция МЭ, позволяющая поддерживать безопасность объектов внутренней области, игнорируя несанкционированные запросы из внешней области. В результате экранирования уменьшается уязвимость внутренних объектов, поскольку первоначально сторонний нарушитель должен преодолеть экран, где защитные механизмы сконфигурированы особенно тщательно и жестко. Кроме того, экранирующая система, в отличие от универсальной, может и должна быть устроена более простым и, следовательно, более безопасным образом, на ней должны присутствовать только те компоненты, которые необходимы для выполнения функций экранирования. Экранирование дает также возможность контролировать информационные потоки, направленные во внешнюю область, что способствует поддержанию во внутренней области режима конфиденциальности. Помимо функций разграничения доступа экраны осуществляют регистрацию информационных обменов.

**«ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ» Руководящий документ Гостехкомиссии РФ**

**Часть 1. Программное обеспечение средств защиты информации**

**КЛАССИФИКАЦИЯ ПО УРОВНЮ КОНТРОЛЯ ОТСУТСТВИЯ НЕДЕКЛАРИРОВАННЫХ ВОЗМОЖНОСТЕЙ**

**Введен в действие Приказом Председателя Гостехкомиссии России № 114 от 4 июня 1999 г.**

Настоящий Руководящий документ (РД) устанавливает классификацию программного обеспечения (ПО) (как отечественного, так и импортного производства) средств защиты информации (СЗИ), в том числе и встроенных в общесистемное и прикладное ПО, по уровню контроля отсутствия в нем недекларированных возможностей.

Действие документа не распространяется на программное обеспечение средств криптографической защиты информации.

Уровень контроля определяется выполнением заданного настоящим РД набора требований, предъявляемого:

>• к составу и содержанию документации, представляемой заявителем для проведения испытаний ПО СЗИ;

>• к содержанию испытаний.

Руководящий документ разработан в дополнение РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (М., Военное издательство, 1992), РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (М., 1992), и РД «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (М., 1997).

Документ предназначен для специалистов испытательных лабораторий, заказчиков, разработчиков ПО СЗИ при его контроле в части отсутствия недекларированных возможностей.

**1. Общие положения**

1.1. Классификация распространяется на ПО, предназначенное для защиты информации ограниченного доступа.

1.2. Устанавливается четыре уровня контроля отсутствия недекларированных возможностей. Каждый уровень характеризуется определенной минимальной совокупностью требований.

1.3. Для ПО, используемого при защите информации, отнесенной к государственной тайне, должен быть обеспечен уровень контроля не ниже третьего.
1.4. Самый высокий уровень контроля — первый, достаточен для ПО, используемого при защите информации с грифом «0В».
Второй уровень контроля достаточен для ПО, используемого при защите информации с грифом «СС».
Третий уровень контроля достаточен для ПО, используемого при защите информации с грифом «С».
1.5 Самый низкий уровень контроля — четвертый, достаточен для ПО, используемого при защите конфиденциальной информации.

**2. Термины и определения**

2.1. Недекларированные возможности — функциональные возможности ПО, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.
Реализацией недекларированных возможностей, в частности, являются программные закладки.
2.2. Программные закладки — преднамеренно внесенные в ПО функциональные объекты, которые при определенных условиях (входных данных) инициируют выполнение не описанных в документации функций ПО, приводящих к нарушению конфиденциальности, доступности или целостности обрабатываемой информации.
2.3. Функциональный объект — элемент программы, осуществляющий выполнение действий по реализации законченного фрагмента алгоритма программы.
В качестве функциональных объектов могут выступать процедуры, функции, ветви, операторы и т. п.
2.4. Информационный объект — элемент программы, содержащий фрагменты информации, циркулирующей в программе. В зависимости от языка программирования в качестве информационных объектов могут выступать переменные, массивы, записи, таблицы, файлы, фрагменты оперативной памяти и т.п.
2.5. Маршрут выполнения функциональных объектов — определенная алгоритмом последовательность выполняемых функциональных объектов.
2.6. Фактический маршрут выполнения функциональных объектов — последовательность фактически выполняемых функциональных объектов при определ1нных условиях (входных данных).
2.7. Критический маршрут выполнения функциональных объектов — такой маршрут, при выполнении которого существует возможность неконтролируемого нарушения установленных правил обработки информационных объектов.
2.8. Статический анализ исходных текстов программ — совокупность методов контроля (не)соответствия реализованных и декларированных в документации функциональных возможностей ПО, основанных на структурном анализе и декомпозиции исходных текстов программ.
2.9. Динамический анализ исходных текстов программ — совокупность методов контроля (не)соответствия реализованных и декларированных в документации функциональных возможностей ПО, основанных на идентификации фактических маршрутов выполнения функциональных объектов с последующим сопоставлением маршрутам, построенным в процессе проведения статического анализа.

**3. Требования к уровню контроля**

3.1. Перечень требований
Требование /Уровень контроля
/4 /3 /2 /1

**Требования к документации**

**I. Контроль состава и содержания документации** / / / /

1.1. Спецификация (ГОСТ 19.202-78) /4- /= /= /=

1.2. Описание программы (ГОСТ 19.402-78) /+/= /= /=

1.3. Описание применения (ГОСТ 19.502-78) /+ /= /= /=

1.4. Пояснительная записка (ГОСТ 19.404-79) /- /+ /= /=

1.5. Тексты программ, входящих в состав по (ГОСТ 19.401-78) /+ /= /= /=

**Требования к содержанию испытаний**

**2. Контроль исходного состояния ПО** /+ /= /= /=

**3. Статический анализ исходных текстов программ** / / / /

3.1. Контроль полноты и отсутствия избыточности исходных текстов /+ /+ /+ /=

3.2. Контроль соответствия исходных текстов ПО его объектному (загрузочному) коду /+ /= /= /+

3.3. Контроль связей функциональных объектов по управлению /— /+ /=/=

3.4. Контроль связей функциональных объектов по информации /- /+ /= /=

Окончание табл.

Требование /Уровень контроля

/4 /3 /2 /1

**Требования к содержанию испытаний**

3.5. Контроль информационных объектов /- /+ /= /=

3.6. Контроль наличия заданных конструкций в исходных текстах /- /- /+ /+

3.7. Формирование перечня маршрутов выполнения функциональных объектов /- /+ /+ /=

3.8. Анализ критических маршрутов выполнения функциональных объектов /- /- /+ /=

3.9. Анализ алгоритма работы функциональных объектов на основе блок-схем, диаграмм и т.п., построенных по исходным текстам контролируемого ПО / / /+ /

4. Динамический анализ исходных текстов программ / / / /

4.1. Контроль выполнения функциональных объектов /- /+ /+ /=

4.2. Сопоставление фактических маршрутов выполнения функциональных объектов и маршрутов, построенных в процессе проведения статического анализа /- /+ /+ /=

5.Отчетность /+ /+ /+ /+

Обозначения:

«-» — нет требований к данному уровню;

«+» — новые или дополнительные требования;

«=» — требования совпадают с требованиями предыдущего уровня.

3.2. Требования к четвертому уровню контроля.

3.2.1. Контроль состава и содержания документации.

В состав документации, представляемой заявителем, должны входить:

>• спецификация (ГОСТ 19.202-78), содержащая сведения о составе ПО и документации на него;

**>•** описание программы (ГОСТ 19.402-78), содержащее основные сведения о составе (с указанием контрольных сумм файлов, входящих в состав ПО), логической структуре и среде функционирования ПО, а также описание методов, приемов и правил эксплуатации средств технологического оснащения при создании ПО;

>• описание применения (ГОСТ 19.502-78), содержащее сведения о назначении ПО, области применения, применяемых методах, классе решаемых задач, ограничениях при применении, минимальной конфигурации технических средств, среде функционирования и порядке работы;

>• исходные тексты программ (ГОСТ 19.401-78), входящих в состав ПО.
Для ПО импортного производства состав документации может отличаться от требуемого, однако содержание должно соответствовать требованиям указанных ГОСТ.
3.2.2. Контроль исходного состояния ПО.
Контроль заключается в фиксации исходного состояния ПО и сравнении полученных результатов с приведенными в документации.
Результатами контроля исходного состояния ПО должны быть рассчитанные уникальные значения контрольных сумм загрузочных модулей и исходных текстов программ, входящих в состав ПО.
Контрольные суммы должны рассчитываться для каждого файла, входящего в состав ПО.
3.2.3. Статический анализ исходных текстов программ.
Статический анализ исходных текстов программ должен включать следующие технологические операции:
>• контроль полноты и отсутствия избыточности исходных текстов ПО на уровне файлов;
>• контроль соответствия исходных текстов ПО его объектному (загрузочному) коду.
3.2.4. Отчетность.
По окончании испытаний оформляется отчет (протокол), содержащий результаты:
>• контроля исходного состояния ПО;
>• контроля полноты и отсутствия избыточности исходных текстов контролируемого ПО на уровне файлов;
>• контроля соответствия исходных текстов ПО его объектному (загрузочному) коду.
3.3. Требования к третьему уровню контроля.
3.3.1. Контроль состава и содержания документации. Требования полностью включают в себя аналогичные требования к четвертому уровню контроля.
Кроме того, должна быть представлена «Пояснительная записка» (ГОСТ 19.404-79), содержащая основные сведения о назначении компонентов, входящих в состав ПО, параметрах обрабатываемых наборов данных (подсхемах баз данных), формируемых кодах возврата, описание используемых переменных, алгоритмов функционирования и т. п.
3.3.2. Контроль исходного состояния ПО. Требования полностью включают в себя аналогичные требования к четвертому уровню контроля.
3.3.3. Статический анализ исходных текстов программ. Кроме аналогичных требований, предъявляемых к четвертому уровню контроля, дополнительно предъявляются следующие требования:
>• контроль полноты и отсутствия избыточности исходных текстов ПО на уровне функциональных объектов (процедур);
>• контроль связей функциональных объектов (модулей, процедур, функций) по управлению;
>• контроль связей функциональных объектов (модулей, процедур, функций) по информации;
>• контроль информационных объектов различных типов (например, локальных переменных, глобальных переменных, внешних переменных и т.п.);
>• формирование перечня маршрутов выполнения функциональных объектов (процедур, функций).
3.3.4. Динамический анализ исходных текстов программ. Динамический анализ исходных текстов программ должен включать следующие технологические операции:
>• контроль выполнения функциональных объектов (процедур, функций);
>• сопоставление фактических маршрутов выполнения функциональных объектов (процедур, функций) и маршрутов, построенных в процессе

проведения статического анализа.
3.3.5. Отчетность.
Кроме аналогичных требований, предъявляемых к четвертому уровню контроля, дополнительно отчет (протокол) должен содержать результаты:
>• контроля полноты и отсутствия избыточности исходных текстов контролируемого ПО на уровне функциональных объектов (процедур);
>• контроля связей функциональных объектов (модулей, процедур, функций) по управлению;
>• контроля связей функциональных объектов (модулей, процедур, функций) по информации;
>• контроля информационных объектов различных типов (например, локальных переменных, глобальных переменных, внешних переменных и т.п.);
>• формирования перечня маршрутов выполнения функциональных объектов (процедур, функций);
>• контроля выполнения функциональных объектов (процедур, функций);
>• сопоставления фактических маршрутов выполнения функциональных объектов (процедур, функций) и маршрутов, построенных в процессе проведения статического анализа.
3.4. Требования ко второму уровню контроля.
3.4.1. Контроль состава и содержания документации. Требования полностью включают в себя аналогичные требования к третьему уровню контроля.
3.4.2. Контроль исходного состояния ПО. Требования полностью включают в себя аналогичные требования к третьему уровню контроля.
3.4.3. Статический анализ исходных текстов программ. Кроме аналогичных требований, предъявляемых к третьему уровню контроля, дополнительно предъявляются следующие требования:
>• контроль полноты и отсутствия избыточности исходных текстов контролируемого программного обеспечения на уровне функциональных объектов (функций);
>• синтаксический контроль наличия заданных конструкций в исходных текстах ПО из списка (базы) потенциально опасных программных конструкций;
>• формирование перечня маршрутов выполнения функциональных объектов (ветвей);
>• анализ критических маршрутов выполнения функциональных объектов (процедур, функций) для заданных экспертом списков информационных объектов;
>• построение по исходным текстам контролируемого ПО блок-схем, диаграмм и т. п. и последующий сравнительный анализ алгоритма работы функциональных объектов (процедур, функций) и алгоритма работы, приведенного в «Пояснительной записке».
3.4.4. Динамический анализ исходных текстов программ.
Кроме аналогичных требований, предъявляемых к третьему уровню контроля, дополнительно предъявляются следующие требования:
>• контроль выполнения функциональных объектов (ветвей);
>• сопоставление фактических маршрутов выполнения функциональных объектов (ветвей) и маршрутов, построенных в процессе проведения статического анализа.
3.4.5 Отчетность.
Кроме аналогичных требований, предъявляемых к третьему уровню контроля, дополнительно отчет (протокол) должен содержать результаты:
>• контроля полноты и отсутствия избыточности исходных текстов контролируемого программного обеспечения на уровне функциональных объектов (функций);
>• синтаксического контроля наличия заданных конструкций в исходных текстах ПО из списка (базы) потенциально опасных конструкций;

>• формирования перечня маршрутов выполнения функциональных объектов (ветвей);
>• анализа критических маршрутов выполнения функциональных объектов (процедур, функций) для заданных экспертом списков информационных объектов;
>• построения по исходным текстам контролируемого ПО блок-схем, диаграмм и т. п., и последующего сравнительного анализа алгоритма работы функциональных объектов (процедур, функций) и алгоритма работы, приведенного в «Пояснительной записке»;
>• контроля выполнения функциональных объектов (ветвей);
>• сопоставления фактических маршрутов выполнения функциональных объектов (ветвей) и маршрутов, построенных в процессе проведения статического анализа.
3.5. Требования к первому уровню контроля.
3.5.1. Контроль состава и содержания документации. Требования полностью включают в себя аналогичные требования ко второму уровню контроля.
3.5.2. Контроль исходного состояния ПО. Требования полностью включают в себя аналогичные требования ко второму уровню контроля.
3.5.3. Статический анализ исходных текстов программ. Кроме аналогичных требований, предъявляемых ко второму уровню контроля, дополнительно предъявляются следующие требования:
>• контроль соответствия исходных текстов ПО его объектному (загрузочному) коду с использованием сертифицированных компиляторов;
>• семантический контроль наличия заданных конструкций в исходных - текстах ПО из списка (базы) потенциально опасных конструкций.
3.5.4. Динамический анализ исходных текстов программ. Требования полностью включают в себя аналогичные требования ко второму уровню контроля.
3.5.5. Отчетность.
Кроме аналогичных требований, предъявляемых ко второму уровню контроля, дополнительно отчет (протокол) должен содержать результаты:
>• контроля соответствия исходных текстов ПО его объектному (загрузочному) коду с использованием сертифицированных компиляторов;
>• семантического контроля наличия заданных конструкций в исходных текстах ПО из списка (базы) потенциально опасных конструкций.

**«ЗАЩИТА ИНФОРМАЦИИ. СПЕЦИАЛЬНЫЕ ЗАЩИТНЫЕ ЗНАКИ. КЛАССИФИКАЦИЯ И ОБЩИЕ ТРЕБОВАНИЯ»**

**Руководящий документ Гостехкомиссии РФ**

**1. Общие положения**

1.1. Настоящий руководящий документ устанавливает классификацию по классам защиты специальных защитных знаков, предназначенных для контроля доступа к объектам защиты, а также для защиты документов от подделки.
1.2. Основными объектами защиты, для которых могут применяться специальные защитные знаки, являются:
>• документированная информация на материальном носителе;
>• специальные почтовые отправления;
>• специальные изделия, технические средства и приборы (в том числе регулируемые и критичные к установке), товары народного потребления, подлежащие опечатыванию и контролю;
>• продукция специального назначения, контейнеры, вагоны, емкости при их перевозке и хранении;
>• помещения, сейфы, запасные выходы, аварийные устройства.
1.3. Документами, защищаемыми с помощью специальных защитных знаков, являются документы, удостоверяющие личность, пропуска сотрудников организаций и учреждений, лицензии, патенты, кредитные карточки, ценные бумаги и т. п.

1.4. Специальные защитные знаки реализуются в виде рисунка, метки, материала, вещества, обложки, ламината, самоклеящейся ленты, отдельных наклеек, самоклеющихся пломб или другого продукта, созданного на основе физико-химических технологий для контроля доступа к объектам защиты, а также для защиты документов от подделки.
1.5. Настоящий документ определяет требования к специальным защитным знакам при их сертификации в Системе сертификации средств защиты информации по требованиям безопасности информации (РООС RU 0001.01БИОО).
1.6. Настоящий документ является руководящим документом для заказчиков специальных защитных знаков и испытательных лабораторий, проводящих сертификационные испытания в Системе сертификации средств защиты информации по требованиям безопасности информации.

**2. Термины и определения**

Специальный защитный знак (СЗЗ) — сертифицированное и зарегистрированное в установленном порядке изделие, предназначенное для контроля несанкционированного доступа к объектам защиты путем определения подлинности и целостности СЗЗ, путем сравнения самого знака или композиции «СЗЗ — подложка» по критериям соответствия характерным признакам визуальными, инструментальными и другими методами.
Несанкционированный доступ (НСД) — нарушение регламентированного доступа к объекту защиты.
Способ изготовления СЗЗ — технологические процессы (приемы и операции, характеризуемые, главным образом, технологическими признаками — последовательностью действий и приемов, их характером, применяемыми режимами, параметрами, инструментами и др.) и материалы (со" ставы и композиции, пасты, пластмассы, лаки, краски и т. д., в том числе полученные химическим путем), используемые для изготовления и производства СЗЗ.
Ноу-хау-технология — совокупность различных технических, коммерческих и других сведений, оформленных в виде технической документации, а также навыков и производственного опыта, необходимых для освоения технологий и методов создания СЗЗ, применяемых в деятельности предприятия или в профессиональной деятельности, доступных определенному кругу лиц. Распространение сведений о ноу-хау-технологиях производства СЗЗ должно быть ограничено соблюдением соответствующих режимных мер.
Идентификация СЗЗ — определение подлинности и целостности СЗЗ по его характерным признакам, а также отсутствия изменений в расположении СЗЗ на объекте защиты или документе путем визуального осмотра или с помощью технических средств общего применения, специализированных технических средств с использованием или без использования специальных методик.
Стойкость защитных свойств СЗЗ — способность к образованию комплекса устойчивых признаков, сигнализирующих о фактах воздействия на СЗЗ или попытке доступа к объекту защиты, а также способность сохранять весь комплекс характерных признаков подлинности и целостности СЗЗ при его регламентированном использовании.
Подлинность СЗЗ — соответствие внешнего вида и наличие в СЗЗ совокупности характерных признаков, предусмотренных техническими условиями.
Целостность СЗЗ — неизменность внешнего вида СЗЗ и совокупности характерных признаков, предусмотренных техническими условиями.

**3. Классификация специальных защитных знаков и общие требования**

3.1. Все СЗЗ делятся на 18 классов. Классификация СЗЗ осуществляется на основе оценки их основных параметров: возможности подделки, идентифицируемости и стойкости защитных свойств.

Класс СЗЗ защищенности /Возможность подделки /Идентифицируемость /Стойкость защитных свойств

1 /A1 /B1 /C1
2 /A1 /B2 /C1
3 /A1 /B3 /C1
4 /A1 /B1 /C2
5 /A1 /B2 /C2
6 /A1 /B3 /C2
7 /A2 /B1 /C1
8 /A2 /B2 /C1
9 /A2 /B3 /C1
10 /A2 /B1 /C2
11 /A2 /B2 /C2
12 /A2 /B3 /C2
13 /A3 /B1 /C1
14 /A3 /B2 /C1
15 /A3 /B3 /C1
16 /A3 /B1 /C2
17 /A3 /B2 /C2
18 /A3 /B3 /C2

**3.2.** Возможность подделки определяется технологией изготовления СЗЗ:

>• A1 — СЗЗ изготовлен с использованием отечественных ноу-хау-технологий;

>• А2 — СЗЗ изготовлен с использованием зарубежных ноу-хау-технологий;

>• А3 — СЗЗ изготовлен без использования ноу-хау-технологий.

3.3. Идентифицируемость определяется уровнем сложности сигнальной информации в знаке:

B1 — целостность и подлинность СЗЗ могут быть однозначно определены с применением специальных технических средств контроля или с помощью приборов или устройств с дополнительной (оптической, компьютерной и т. п.) обработкой сигнала по специальной методике, основанной на технологии изготовления СЗЗ;

82 — целостность и подлинность СЗЗ могут быть однозначно определены на основании специальных методик контроля без применения технических средств контроля или с использованием серийно выпускаемых технических средств;

83 — целостность и подлинность СЗЗ могут быть однозначно определены визуально без применения технических средств и специальных методик контроля.

3.4. По стойкости защитных свойств СЗЗ подразделяются на две группы:

>• C1 — в технических условиях на СЗЗ задано изменение его внешнего вида и хотя бы одного характерного признака при несанкционированных воздействиях на СЗЗ или нарушении условий его эксплуатации;

>• С2 — в технических условиях на СЗЗ задано изменение только его внешнего вида при несанкционированных воздействиях на СЗЗ или нарушении условий его эксплуатации.

3.5. Для защиты информации, отнесенной к государственной тайне, и защиты технических средств категорированных объектов используются только СЗЗ, сертифицированные по классу не ниже 6:

>• по классам 1 и 2 — для защиты объектов 1-й категории и информации соответствующей степени секретности;

**>•** по классам 3 и 4 — для защиты объектов 2-й категории и информации соответствующей степени секретности;

>• по классам 5 и 6 — для защиты объектов 3-й категории и информации соответствующей степени секретности.

Использование СЗЗ, сертифицированных по классам 7—12, допускается только для защиты объектов 3-й категории и информации соответствующего

уровня секретности при обеспечении дополнительных организационно-технических мер защиты, согласованных с Гостехкомиссией России.
3.6. При нарушении режима сохранения информации о применяемой ноу-хау-технологии, изменении условий производства и т. п. использование СЗЗ запрещается, ранее выданный сертификат аннулируется.

## 2.2. Организация защиты информации

### 2.2.1. Основные понятия информационной безопасности

После знакомства с некоторыми правовыми актами, которые регулируют (или по крайней мере должны регулировать) деятельность тех лиц, чья сфера интересов находится в области защиты информации или ее съема, вернемся к тому вопросу, с которого начали эту книгу. Что же все-таки такое концепция информационной безопасности? Громкое название этого мероприятия никого не должно вводить в заблуждение. Если отбросить научную, а скорее околонаучную фразеологию, то концепция информационной безопасности как система взглядов на цели, способы обеспечения безопасности информации и средства ее защиты должна в общем виде отвечать на три простых вопроса: что защищать; от чего защищать; как защищать?
С вопросом «что защищать?» связано понятие «объект защиты». Этот вопрос может вызвать недоумение: ясно, что речь идет об информации, значит ее и нужно защищать. А в нашем случае это набор определенных сведений. Но тут всплывает одно из главных свойств информации, вытекающее из самой ее природы. Ее феномен в том, что в физическом, а не в философском плане она подразумевает свой носитель, то есть выражение «получить доступ к информации» следует понимать, как получение доступа к вполне определенному носителю. Это может быть подслушанный разговор, украденный документ, перехваченный факс, выпотрошенный компьютер и т. д. О каналах утечки информации мы подробно говорили в разделе 1.2.
Поэтому под объектом защиты будем подразумевать не абстрактное понятие, а комплекс физических, аппаратных, программных и документальных средств, предназначенных для сбора, передачи, обработки и хранения информации.
Ключевое свойство информации — ее ценность, то есть для нашего случая стоимость ущерба от разрушения, потери или разглашения. Кроме того, спецификой информации является то, что она не исчезает при потреблении, не передается полностью при обмене (в отличие от денег остается и у старого пользователя). С одной стороны, она является неделимой и имеет смысл только при достаточно полном объеме сведений, с другой — качество ее повышается при добавлении новых достоверных данных, то есть можно проводить постепенное накапливание сведений и небольшими частями.
Поэтому, прежде чем ответить на первый вопрос, все-таки необходимо четко разобраться, какая информация потребует защиты. Это может быть, например, весь объем данных, накапливающийся и формирующийся в фирме, которые имеют коммерческую значимость. Сведения о количестве выпускаемой продукции и об объемах продаж. Сведения о поставщиках и производителях, продавцах и дилерах, договорах и клиентах. Планы фирмы, предельные цены, размеры премий дилерам и посредникам, имена и адреса сотрудников. Себестоимость продукции, маркетинговые и аналитические исследования. Финансовое состояние фирмы, размеры оплаты труда, денежный наличный оборот, особенно каналы движения денежной массы. Это могут быть какие-нибудь деловые (или не очень деловые — типа экс-министра В. Ковалева или «человека, похожего на Генерального прокурора

Ю. Скуратова») встречи, детали частной жизни и т. д. В каждом отдельном случае нужно тщательно проанализировать: какая конкретная информация может оказаться совершенно нежелательной для огласки. Затем аккуратно привязать эту информацию к носителям. Допустим, если проводятся короткие устные переговоры, без оформления каких-либо документов, то в качестве объекта защиты выступает только сам разговор. Если привлечены какие-нибудь технические средства связи, записи или составляются какие-либо документы, то количество объектов существенно возрастает.

Следующим шагом должна стать их ранжировка по степени ценности содержащейся информации (ведь такие объекты защиты, как разговор и итоговый документ — это «две большие разницы»). И наконец, производится определение потенциально опасных систем, позволяющих получить доступ к этим объектам. В проведении этого этапа работы неплохо могут помочь материалы, содержащиеся как в табл. 1.1.1, так и в первой части данной книги. Поэтому все описанные средства несанкционированного съема информации и привязаны к конкретному носителю, для работы с которым они предназначены. Проделав это простое исследование, можно практически ответить на первый вопрос. Поверьте, если «исследователь» хоть в общих чертах знаком с основными методами работы злоумышленников и возможностями их аппаратуры, то работа не займет много времени.

Вопрос «от чего защищаться?» связан с понятием «угроза». Угроза — потенциальная возможность неправомерного преднамеренного или случайного воздействия на объект защиты, приводящее к потере или разглашению информации. Обычно выделяют внутренние и внешние источники угроз.

К внутренней угрозе относятся как преднамеренные действия, так и непреднамеренные ошибки персонала (не зря говорят: «Простота хуже воровства»). Сразу предупреждаем, что этот сложнейший вопрос выходит за рамки данной книги, здесь нужны специалисты совсем другого профиля.

Внешние угрозы весьма разнообразны. В условиях рыночной экономики, когда существует реальная конкуренция между организациями, у них возникает интерес к деятельности соперничающих фирм. Целью этого интереса является добывание информации, относящейся к сфере коммерческой тайны, то есть о замыслах, финансовом состоянии, клиентах, ценах и т. д. Получение такой информации и ее использование конкурентами (да и некоторыми партнерами) может причинить существенный ущерб фирме. Как уже говорилось выше, имеется достаточно развитый рынок услуг по добыванию информации такого рода. Например, в Санкт-Петербурге целый ряд частных детективных агентств, негласно, конечно, специализируется именно на этом поприще. Есть они и в других крупных городах. Притом, некоторые из них оснащены на достаточно высоком уровне и берутся за любую работу. В частности, уже отмечалось, что московская охранная фирма «Атолл» выполняла заказы по сбору компромата даже на семью президента.

Иногда грешат и сами бизнесмены, начитавшиеся плохих детективов. Сотрудникам Лаборатории ППШ приходилось сталкиваться и с этими любителями, притом не только с радистами по образованию, а с инженерами-химиками, юристами, студентами всевозможных профилей и даже одним довольно известным музыкантом, возомнившими себя Джеймсами Бондами, но «вычисленными» буквально за считанные часы. Правда, есть и среди любителей исключения. В телевизионной программе «Совершенно секретно» был показан доморощенный Кулибин, сделавший своими руками автоматизированный комплекс для контроля каналов сотовой связи и за весьма скромную плату предоставлявший заинтересованным лицам записи всех как входящих, так и исходящих звонков. Для «заказа клиента» надо было только сообщить его номер. ФСБ, прикрывшая этот бизнес, по достоинству «оценила» самородка.

Помимо конкурентов серьезную угрозу некоторым фирмам или частным лицам

могут представлять мафиозные группировки. «Братва» в последнее время все больше внимания уделяет получению информации по техническим каналам. Для этого создаются небольшие организации из доверенных людей, на обучение и экипировку которых не скупятся. Например, прошедший в 1997 году в Санкт-Петербурге процесс над бандой одного из главных рэкетиров города по кличке Пудель, отколовшегося от Тамбовской группировки, показал, что в составе его группы было прекрасно оснащенное подразделение, занимающееся сбором коммерческой информации с помощью технических средств. Прежде чем «наехать» на фирму, рэкетир тщательно изучал ее деятельность и состояние финансов, а затем выставлял «научно обоснованный счет». В феврале 1999 года в прессе появилось сообщение о том, что в Интернете на печально известном сайте «Коготь» предоставляется очень необычная информация, а именно — расшифровки подслушанных телефонных разговоров, перехваченных пейджинговых сообщений и даже оперативные справки на многих известных людей: В. Рушайло, А. Коха, В. Степашина, Ю. Скуратова. Это явный ответ на заявление правительства об усилении борьбы с организованной преступностью.

Многие крупные коммерческие структуры создали собственные мощные службы безопасности, одной из главных задач которых, в условиях нашего специфического рынка, является добывание информации о потенциальных клиентах, партнерах или конкурентах. При этом часто не считается зазорным внедрение к подопечным людей или специальной техники.

Они же очень жестко вынуждены контролировать свой персонал с целью недопущения утечки информации о собственных коммерческих секретах. Техническому оснащению и квалификации сотрудников безопасности отдельных «богатеньких» фирм иногда могут позавидовать даже государственные спецслужбы.

Нельзя забывать, что интеграция России в международные организации, участие в интернациональных проектах, колоссальный советский научный и технологический «задел» в целом ряде направлений делает отечественных предпринимателей объектом пристального внимания частных и даже государственных служб разведки Запада и Востока. Правда, в самой России им пока развернуться особенно не дают, но многочисленные скандалы, связанные с высылкой пойманных за руку иностранных граждан, невольно настораживают.

И наконец, собственные спецслужбы. Многие предприниматели, да и простые граждане, считают, что их переговоры, особенно с помощью телефона, постоянно записываются спецслужбами. Этому убеждению в немалой степени способствует абсолютно некомпетентная информация, часто появляющаяся на страницах нашей периодической печати, вполне определенной направленности. Простые логические рассуждения показывают, что Тотальный контроль хотя бы за телефонными переговорами не в состоянии организовать ни одно государство мира. С другой стороны, спецслужбы всех стран, конечно, ведут выборочное прослушивание отдельных лиц. В разделах 1.1 и 2.1 приведена законодательная основа для проведения такого рода мероприятий.

Согласно «Совместному решению по эксплуатационно-техническим требованиям к средствам и сетям электросвязи для обеспечения оперативно-розыскных мероприятий», в состав этих сетей, независимо от формы собственности, вводятся аппаратные и программные средства контроля, позволяющие подключаться к любым абонентским линиям. Достаточно подробно с этим документом можно ознакомиться в газете «Час Пик» (№ 8, 1993 год). Кроме такой стационарной аппаратуры в арсенале спецслужб и правоохранительных органов большое количество и других технических систем. Если верить некоторым детективам, то эти системы обладают совершенно невероятными возможностями, однако аппаратура

используется весьма обычная, может несколько более высокого качества, чем та, что описана в этой книге, а сам необычный результат получается лишь вследствие высочайшего профессионализма тех, кто ее практически применяет.

Для иллюстрации этой простой мысли позволим себе привести небольшую выдержку из книги В. А. Стрелецкого «Мракобесие» (М.; Детектив-Пресс, 1998). Полковник Стрелецкий — бывший начальник отдела «П» (борьба с коррупцией) Службы безопасности президента (СБП) и главный организатор задержания пресловутой коробки и>•под «Ксерокса», выносимой в 1996 году из Белого дома. На странице 248 можно прочитать: «... 6 ноября 1996 года "Московский Комсомолец" опубликовал стенограмму переговоров Чубайса и Илюшина. Разразившийся вслед за публикацией скандал был опровергнут Чубайсом — мол, переговоры не вел, все ложь и клевета. Тогда были представлены пленки записи... Закон об оперативно-розыскной деятельности давал нам право разрабатывать любого гражданина РФ. Его должность роли не играет... Из источников в его (Чубайса. — Прим. авт.) окружении я узнал, что 22 июня он должен приехать к первому помощнику президента В. Илюшину в «Президент-Отель», чтобы обсудить ситуацию. Негласный доброжелатель согласился нам помочь. Мы договорились, что он установит в кабинете Илюшина диктофон, а потом незаметно заберет технику обратно. Результаты превзошли все ожидания». Как видите, пожалуй, самая «крутая» российская спецслужба воспользовалась самым простым техническим устройством, но с максимальным эффектом.

Поэтому той категории читателей, которые задумали нарушить закон, уклониться от уплаты налогов, заняться контрабандой или иным образом попасть в зону внимания правоохранительных органов, советуем хорошенько подумать прежде, чем делать это и еще раз внимательно прочитать материалы первой части данной книги. Поверьте, чтобы «достать» преступника — у спецслужб широчайший арсенал средств. А законопослушным гражданам надо тщательно изучить раздел 2.1, где приведена основная нормативно-правовая база защиты информации, и спокойно работать, не обращая внимания на досужие домыслы некоторых «рыцарей пера». Пока человек в ладу с законом, угроз его коммерческим тайнам и личной жизни со стороны правоохранительных органов опасаться не следует.

После того, как были проанализированы потенциальные угрозы, надо выбрать из них действительно реальные, исходя из сферы деятельности и ценности информации. Если кто-то сделает вывод, что он, как тот Неуловимый Джон из анекдота, никому не нужен, тогда пусть эта книга для него станет просто занимательным чтением для повышения общей эрудиции.

Если ответ на вопрос «от чего защищать?», все же выявит заинтересованных лиц, то надо объективно оценить их возможности и составить примерный перечень средств, особенно технических, которые могут быть применены. Тут очень важно не переоценить противника, иначе это выльется в совершенно лишние затраты, поэтому на этом этапе лучше проконсультироваться у специалистов. Сотрудники Лаборатории ППШ могут привести много примеров, когда бесплатная 15-минутная консультация спасала от многотысячных затрат. Вместе с тем, хотим предупредить тех, кто не в ладу с законом, если собираетесь обеспечить защиту вашей информации от спецслужб, то это дело практически безнадежное, поскольку любителям такая проблема не по зубам, а если захотите обратиться к истинным профессионалам, то хорошенько подумайте: из кого комплектуется штат таких организаций. В лучшем случае, клиент получит вежливый отказ.

Теперь осталось ответить только на последний вопрос.

С вопросом «как защищать?» связано понятие «система защиты». Система защиты — это комплекс мер и средств, а также деятельность на их основе, направленная на выявление, отражение и ликвидацию различных видов угроз безопасности объектов защиты. Принято различать следующие основные виды

средств защиты: нормативно-правовые; морально-этические; организационные; технические.

Нормативно-правовые — включают в себя законы и другие правовые акты, а также механизмы их реализации, регламентирующие информационные отношения в обществе. Эти вопросы достаточно подробно изложены в разделе 2.1. Несколько обособленно стоит проблема лицензирования, но и она кажется близка к решению. Впервые в истории российского государства регулирование отношений, возникающих в процессе работы с закрытой информацией, на законодательном уровне было определено Законом РФ от 21.09.93 г. «О государственной тайне». Одним из базовых положений этого закона является лицензирование деятельности предприятий, учреждений и организаций по допуску к проведению работ, связанных с созданием средств защиты информации, а также осуществлению мероприятий и (или) оказанию услуг по ее защите (статья 27). Координация деятельности всех подобных организация возложена на Межведомственную комиссию по защите государственной тайны. Положение об этой комиссии утверждено указом Президента России от 20.01.96 г. № 71.

Организация лицензионной деятельности органически сочетается с общей системой лицензирования, определенной Положением правительства РФ от 24.12.94 г. № 1418. Сам порядок лицензирования в области защиты информации определен «Положением о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и/или оказанием услуг по защите государственной тайны». Данным Положением определены органы, уполномоченные на ведение лицензионной деятельности:

>• ФСБ [Лицензируемые виды деятельности: допуск к проведению работ, связанных с использованием сведений, составляющих государственную тайну (на территории РФ), на право осуществления мероприятий и (или) оказанием услуг в области защиты государственной тайны; на право проведения работ, связанных с созданием средств защиты информации; на право разработки, производства, продажи и т. п. специальных технических средств негласного получения информации];

>• Гостехкомиссия России [Лицензируемые виды деятельности: на право осуществления мероприятий и/или оказанием услуг в области защиты государственной тайны (противодействие ИТР, защита информации); на право проведения работ, связанных с созданием средств защиты информации от несанкционированного доступа); на право

СЕРИЯ ЛГ 0002 НОМЕР 000066

ЛИЦЕНЗИЯ

Регистрационный номер 30 от "28" декабря 1998 г.

НА ДЕЯТЕЛЬНОСТЬ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

Государственная техническая комиссия при Президенте Российской Федерации разрешает выполнять работы (оказывать услуги) по защите информации, указанные в пунктах

1.2; 2; 3.1; 3.4-3.9; 4; 5а-в; 6.

настоящей Лицензии на всей территории Российской Федерации (виды работ см. на обороте бланка Лицензии).

Лицензия выдана Военному инженерно-космическому университету имени А.Ф.Можайского

197082, г.Санкт-Петербург, Ждановская наб., дом 13

код ОКПО - 07726295

Лицензия действительна до "28 декабря 2001 г.

Условия осуществления работ (оказания услуг) в соответствии с НТД Гостехкомиссии России

ПЕРВЫЙ ЗАМЕСТИТЕЛЬ ПРЕДСЕДАТЕЛЯ ГОСТЕХКОМИССИИ РОССИИ

В.С.Соколов

Лицензия продлена до " " 19 г.

М.П.

**Рис. 2.2.1. Лицензия, выдаваемая Гостехкомиссией России на право осуществления мероприятий в области защиты государственной тайны (противодействия ИТР, защиты информации)**

***

**Федеральное государственное унитарное предприятие Научно-производственное предприятие «ГАММА»**

117420, Москва, ул. Профсоюзная, 78 Тел. (095) 128-69-93, факс (095) 330-33-88

**Представительство в Санкт-Петербурге:**

197110, Санкт-Петербург, ул. Пионерская, 44 Тел/факс (812) 235-55-18;

м. т. 26-05

**Лицензии ФГУП НПП «Гамма»:**

ФАПСИ № ЛФ/13-101 от 30.04.97 г. на проведение специальных проверок и специальных исследований. Гостехкомиссии № 82 от 25.07.98 г.

ФСБ № 657 от 31.03.97 г.

Аттестат аккредитации органа по аттестации № СЗИ RU.082B 29.040

Федеральное государственное унитарное предприятие Научно-производственное предприятие «Гамма» работает в области защиты информации около 30 лет, являясь правопреемником спецподразделения НИИ Автоматической аппаратуры, имеет многолетний опыт проведения работ по комплексной защите информации на объектах АСУ и ЭВТ.

Предприятие производит специальные работы в Администрации Президента РФ, Государственной Думе и Совете Федерации, в ряде министерств и ведомств Российской Федерации, на многих крупнейших предприятиях.

Специалистами предприятия разработаны действующие методики проведения специальных исследований, а также ведутся работы по их совершенствованию.

В настоящее время в ФГУП НПП «Гамма» работает более 50 сотрудников. Все рабочие группы укомплектованы выпускниками таких ведущих вузов страны, как МИФИ, МФТИ, МИРЭА, МЭИС, ВИКА им. А. Ф. Можайского. На счету наших сотрудников десятки авторских свидетельств, сотни печатных работ, несколько защищенных кандидатских диссертаций.

Предприятие аккредитовано в качестве органа по сертификации средств защиты информации по требованиям безопасности информации для проведения аттестации объектов информатизации.

Предприятие осуществляет деятельность практически во всех областях защиты информации и приглашает к сотрудничеству заинтересованные предприятия и организации.

***

проведения работ, связанных с созданием средств защиты информации] (внешний вид такой лицензии показан на рис. 2.2.1);

>• ФАПСИ [Лицензируемые виды деятельности: на право осуществления мероприятий и (или) оказанием услуг в области защиты государственной тайны (противодействие ИТР, защита информации от несанкционированного доступа); на право проведения работ, связанных с созданием средств защиты информации];

>• Служба внешней разведки [Лицензируемые виды деятельности: допуск к проведению работ, связанных с использованием сведений, составляющих государственную тайну (за рубежом); на право осуществления мероприятий и/или оказанием услуг в области защиты государственной тайны (режим секретности, противодействие ИТР, защита информации от несанкционированного доступа); на право проведения работ, связанных с созданием средств защиты информации];

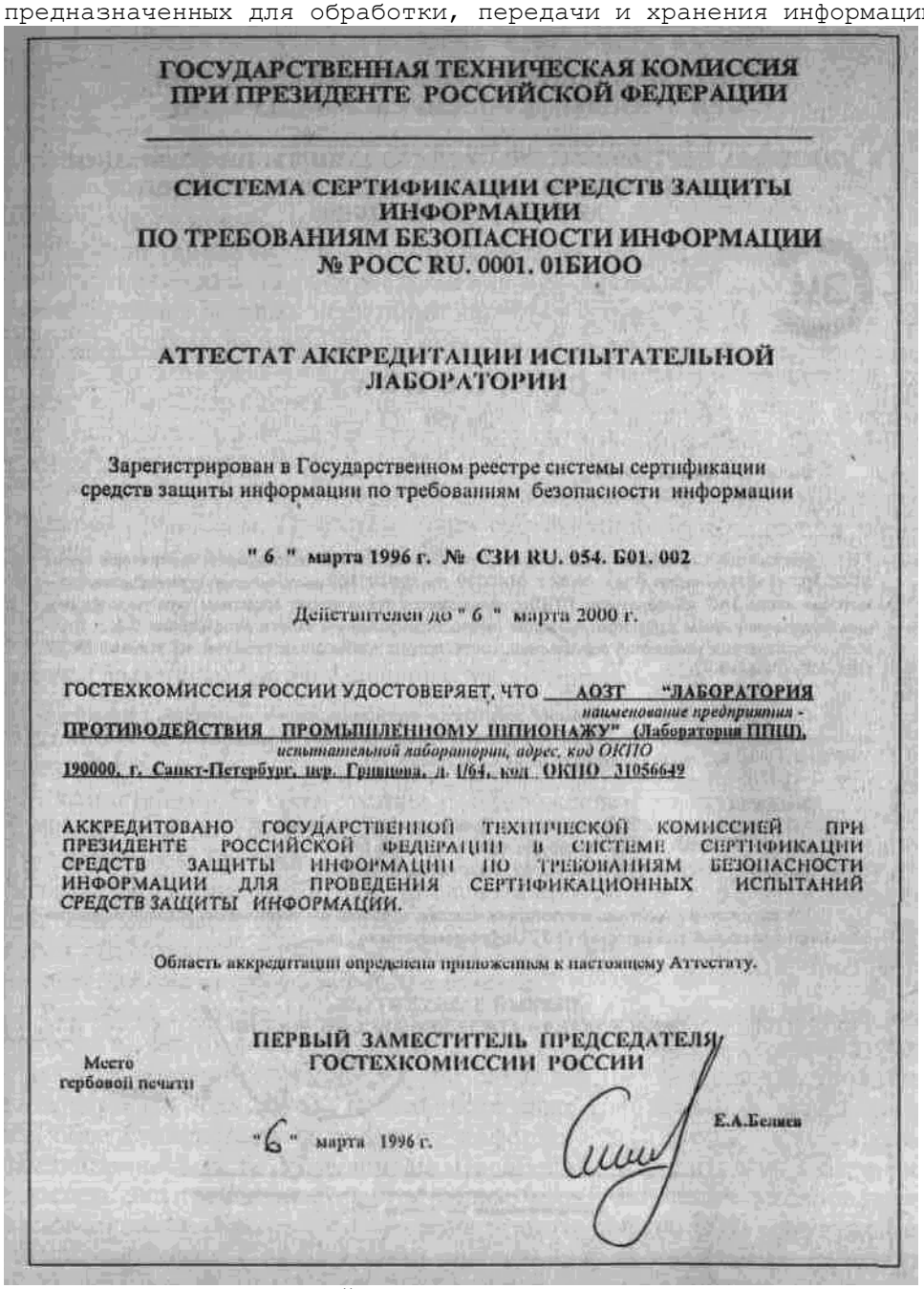
>• Минобороны [Лицензируемые виды деятельности: на право проведения работ, связанных с созданием средств защиты информации].

В свою очередь, уполномоченные органы могут создавать аттестационные центры (региональные или отраслевые) по соответствующим направлениям деятельности. Если предприятие собирается развернуть деятельность на ниве защиты информации, то оно обязано подать заявление в уполномоченную организацию, которая, в свою очередь, дает аттестационному центру соответствующее поручение на проведение специальной экспертизы.

Результаты работы экспертной комиссии оформляются актом. Акт прилагается к заявлению о выдаче лицензии и направляется в уполномоченный орган, где и принимается окончательное решение. Срок действия лицензии устанавливается в зависимости от рода деятельности, но не менее 3-х и не более 5 лет. На каждый вид деятельности выдается

отдельная лицензия.
Таким образом, если необходима действительно квалифицированная помощь, то лучше обращаться только в организации, имеющие лицензию. А теперь «информация к размышлению» для «информационных пиратов»:
подготовлены предложения об установлении административной ответственности за проведение работ в области защиты информации без лицензии или с нарушением условий лицензии. Эти предложения представлены в Государственную Думу с просьбой об их включении в Кодекс РФ об административных нарушениях.
Морально-этические — нормы и правила поведения, направленные на обеспечение безопасности информации, не закрепленные законодательно или административно, но поддерживаемые в коллективах через традиции и механизм общественного мнения. В данной книге мы не будем касаться этих вопросов. Самое главное, что надо сделать для поддержания соответствующего настроя: во-первых, создать здоровый дружный коллектив, а во-вторых, дать своим сотрудникам хотя бы минимум знаний о мерах информационной безопасности. Нам приходилось наблюдать ситуации, когда руководство фирмы просит проверить помещение на наличие подслушивающих устройств, а в это время один из вице-президентов в курилке, кстати общей для нескольких организаций, хвастается выгодной сделкой, описывая весьма «интересные» детали.
Организационные — правила, меры и мероприятия, регламентирующие вопросы доступа, хранения, применения и передачи информации, вводимые в действие административным путем. Подробно этот материал изложен в подразделе 2.2.2. Скажем только, что установка любых, самых дорогих, технических средств защиты обернется пустой тратой денег для организации, в которой не решены на должном уровне организационные вопросы. И это справедливо для любых каналов утечки. Конечно, введение разного рода ограничений — работа не из самых приятных, но это может дать весьма ощутимый эффект и значительно сэкономить средства. Особенно, если проведенный анализ (что защищать и от кого защищать) показал полное отсутствие угрозы от серьезной организации, способной использовать сложные технические средства или нанять «крутую» фирму.
Технические средства — комплексы специального технического и программного обеспечения, предназначенные для предотвращения утечки обрабатываемой или хранящейся у вас информации путем исключения несанкционированного доступа к ней с помощью технических устройств съема. Эти средства подробно описаны во второй части книги. В этом разделе остановимся только на вопросах сертификации аппаратуры такого рода, которые не менее актуальны, чем лицензирование. С принятием комплекса законодательных и иных нормативных актов правового регулирования в области сертификации средств защиты информации проблема обеспечения качества используемых для этих целей средств встала на прочную правовую основу.
«Положением о сертификации средств защиты информации», утвержденным постановлением Правительства РФ № 608 от 26.07.95 г., определено 5 систем сертификации. В Государственном реестре Госстандарта зарегистрированы соответственно:
>• ФАПСИ с системой сертификации средств криптографической защиты информации;
>• Гостехкомиссия с системой сертификации средств защиты по требованиям безопасности информации;
>• Минобороны с системой сертификации средств защиты, относящимся к его компетенции.
Работы по созданию других систем сертификации на момент написания книги пока не завершены. Системы предусматривают обязательную сертификацию технических, программно-технических и программных средств,

предназначенных для обработки, передачи и хранения информации



ГОСУДАРСТВЕННАЯ ТЕХНИЧЕСКАЯ КОМИССИЯ
ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ
ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU. 0001. 01БИОО

АТТЕСТАТ АККРЕДИТАЦИИ ИСПЫТАТЕЛЬНОЙ ЛАБОРАТОРИИ

Зарегистрирован в Государственном реестре системы сертификации средств защиты информации по требованиям безопасности информации

" 6 " марта 1996 г. № СЗИ RU. 054. Б01. 002

Действителен до " 6 " марта 2000 г.

ГОСТЕХКОМИССИЯ РОССИИ УДОСТОВЕРЯЕТ, ЧТО АОЗТ "ЛАБОРАТОРИЯ
*наименование предприятия -*
ПРОТИВОДЕЙСТВИЯ ПРОМЫШЛЕННОМУ ШПИОНАЖУ" (Лаборатория ППШ),
*испытательной лаборатории, адрес, код ОКПО*
190000, г. Санкт-Петербург, пер. Гривцова, д. 1/64, код ОКПО 31056649

АККРЕДИТОВАНО ГОСУДАРСТВЕННОЙ ТЕХНИЧЕСКОЙ КОМИССИЕЙ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ В СИСТЕМЕ СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ДЛЯ ПРОВЕДЕНИЯ СЕРТИФИКАЦИОННЫХ ИСПЫТАНИЙ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ.

Область аккредитации определена приложением к настоящему Аттестату.

ПЕРВЫЙ ЗАМЕСТИТЕЛЬ ПРЕДСЕДАТЕЛЯ
ГОСТЕХКОМИССИИ РОССИИ

Место гербовой печати

"6" марта 1996 г.

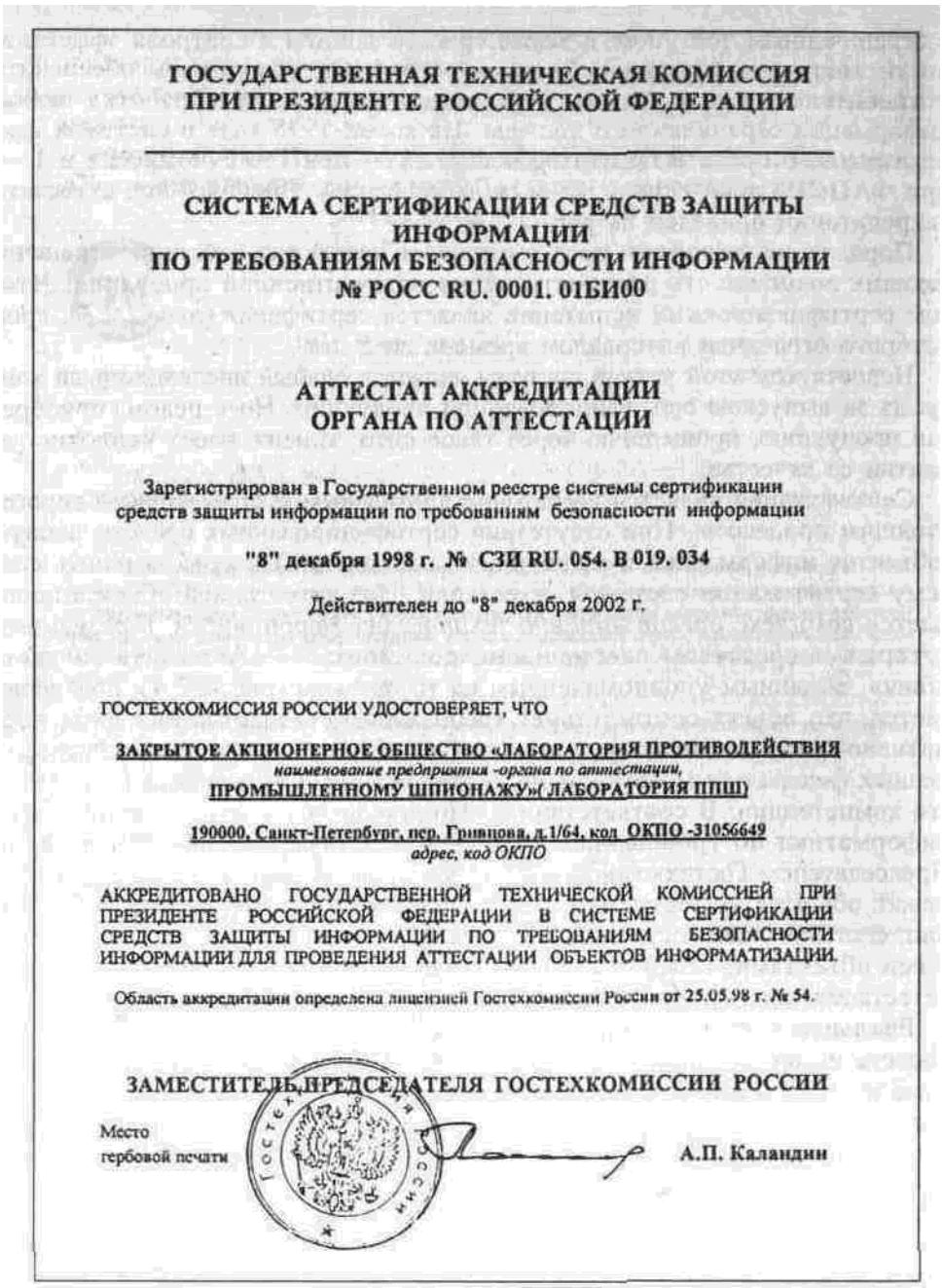
Е.А.Белаев

**Рис. 2.2.2. Внешний вид аттестата аккредитации испытательной лаборатории, выданный Гостехкомиссией России**

с ограниченным доступом, а также средств защиты и контроля эффективности защиты информации. Системы сертификации призваны обеспечить потребителю средств защиты информации безопасную обработку любой информации ограниченного доступа. На конец 1998 года в системах аккредитовано 6 органов по сертификации (5 — при Гостехкомиссии и 1 — при ФАПСИ) и 46 испытательных лабораторий. Внешний вид аттестата аккредитации приведен на рис. 2.2.4.

Порядок сертификации предусматривает целый ряд действий, ограничивающих возможность распространения некачественной продукции. Итогом сертификационных испытаний является сертификат (рис. 2.2.3), срок

которого ограничен интервалом времени до 5 лет.
Недостатком этой четкой системы является слабый инспекционный контроль за выпуском сертифицированной продукции. Но в целом, приобретая продукцию, прошедшую через такое сито, клиент имеет неплохие гарантии ее качества.
Сертификация является достаточно длительным и относительно дорогостоящим процессом. При отсутствии сертифицированных средств защиты (объектов информатики в защищенном исполнении) можно заменить систему сертификации системой аттестации. Под аттестацией объекта понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа — «Аттестата соответствия», выданным уполномоченным на то органом (рис. 2.2.4), подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных федеральным органом по сертификации и аттестации в пределах его компетенции. В соответствии с «Положением по аттестации объектов информатики по требованиям безопасности информации» (Утверждено Председателем Гостехкомиссии 25.11.94 г.) обязательной аттестации подлежат объекты информатики, предназначенные для обработки информации, составляющей государственную тайну, управления экологически опасными объектами, ведения секретных переговоров. В остальных случаях аттестация носит добровольный характер.
Реальная система защиты включает в себя все перечисленные виды средств и, как правило, создается путем их интеграции. Главной трудностью в ее создании является то, что одновременно она должна удовлетворять двум группам прямо противоположных требований. С одной стороны, обеспечивать надежную защиту информации. С другой — не создавать заметных неудобств сотрудникам и особенно потребителям. Обычно совместить эти требования удается только достаточно квалифицированному профессионалу. Кроме того, система защиты должна быть адекватна возможным угрозам, с обязательной оценкой как вероятности их появления, так и величины реального ущерба от потери или разглашения информации, циркулирующей в определенном носителе.



ГОСУДАРСТВЕННАЯ ТЕХНИЧЕСКАЯ КОМИССИЯ
ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ
ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU. 0001. 01БИ00

АТТЕСТАТ АККРЕДИТАЦИИ
ОРГАНА ПО АТТЕСТАЦИИ

Зарегистрирован в Государственном реестре системы сертификации средств защиты информации по требованиям безопасности информации

"8" декабря 1998 г. № СЗИ RU. 054. В 019. 034

Действителен до "8" декабря 2002 г.

ГОСТЕХКОМИССИЯ РОССИИ УДОСТОВЕРЯЕТ, ЧТО

ЗАКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО «ЛАБОРАТОРИЯ ПРОТИВОДЕЙСТВИЯ
*наименование предприятия -органа по аттестации,*
ПРОМЫШЛЕННОМУ ШПИОНАЖУ»( ЛАБОРАТОРИЯ ППШ)

190000, Санкт-Петербург, пер. Гривцова, д.1/64, код ОКПО -31056649
*адрес, код ОКПО*

АККРЕДИТОВАНО ГОСУДАРСТВЕННОЙ ТЕХНИЧЕСКОЙ КОМИССИЕЙ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ В СИСТЕМЕ СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ДЛЯ ПРОВЕДЕНИЯ АТТЕСТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ.

Область аккредитации определена лицензией Гостехкомиссии России от 25.05.98 г. № 54.

ЗАМЕСТИТЕЛЬ ПРЕДСЕДАТЕЛЯ ГОСТЕХКОМИССИИ РОССИИ

Место гербовой печати

А.П. Каландин

**Рис. 2.2.4. Внешний вид аттестата аккредитация органа по аттестация информатизации, выданный Гостехкомиссией России**


**190000, РОССИЯ, САНКТ-ПЕТЕРБУРГ, ПЕР. ГРИВЦОВА, 1/64;**
**ТЕЛ. +7 (812) 219-1137, 314-2259;**
**ФАКС: +7 (812) 315-8375 E-MAIL: POSTMASTER@PPS.SPB.SU URL: http://www.pps.ru**


**Информация о фирме**

Основным видом деятельности **Лаборатории ППШ** является проведение комплекса организационных и технических мероприятий по защите важной

информации от несанкционированного доступа. Под этим понимается **полное комплексное обследование помещений** с целью выявления всех возможных технических каналов утечки информации, разработка рекомендаций по закрытию выявленных каналов и проведению необходимых организационных и технических мероприятий, подготовка перечня рекомендуемого оборудования и его поставка.

Другими видами деятельности **Лаборатории ППШ** являются:

=> проведение сертификационных испытаний и исследований в рамках системы сертификации средств защиты информации по требованиям безопасности информации;

=> проведение комплекса мероприятий по защите информации **в АС;**

=> аттестация средств и систем информатизации на соответствие требованиям по защите информации;

=> проведение специсследований средств ЭВТ в соответствии с требованиями и по методикам Гостехкомиссии РФ;

=> проведение исследований и разработок в области технических средств защиты информации;

=> производство, поставка и реализация специального оборудования;

=> консультации и обучение по различным вопросам безопасности и защиты информации.

Все перечисленные виды деятельности **Лаборатория ППШ осуществляет** на основании следующих документов:

• «Лицензия на деятельность в области защиты информации» № 54 от 26 мая 1995 г. по пунктам 2-6 (в полном объеме), выданная Государственной технической комиссией при Президенте Российской Федерации (продлена до 2001 года);

• «Аттестат аккредитации испытательной лаборатории» в системе сертификации средств защиты информации по требованиям безопасности информации

№ СЗИ RU.054.B01.002 от 6 марта 1996 г.

• Лицензия УФСБ России № 241 от 14 июля 1997 г.

• «Аттестат аккредитации органа по аттестации» в системе сертификации средств защиты информации по требованиям безопасности информации Ms СЗИ RU.054.B019.034 от 8 декабря 1998 г.

После выбора системы защиты остается сделать последний шаг: составить соответствующий перечень (набор) средств конкретной их реализации, которые наиболее полно ликвидируют потенциальную угрозу. Напомним, что угроза считается ликвидированной, если затраты на преодоление защиты превысят стоимость защищаемой информации.

### 2.2.2. Организационные мероприятия по защите информации

Как говорилось выше, защита информации — есть комплекс мероприятий, проводимых собственником информации, по ограждению своих прав на владение и распоряжение информацией, созданию условий, ограничивающих ее распространение и исключающих доступ к засекреченной информации и ее носителям.

Следовательно, под защитой информации следует также понимать обеспечение безопасности информации и средств информации, в которых накапливается, обрабатывается и хранится защищаемая информация.

Таким образом, защита информации — это деятельность собственника информации или уполномоченных им лиц по:

>• обеспечению своих прав на владение, распоряжение и управление защищаемой информацией;

>• предотвращению утечки и утраты информации;

сохранению полноты, достоверности, целостности защищаемой информации, ее массивов и программ обработки;

>• сохранению конфиденциальности или секретности защищаемой информации в соответствии с правилами, установленными законодательными и другими

нормативными актами.
Система защиты сведений, отнесенных к коммерческой тайне, и их носителей складывается из:
>• органов защиты коммерческой тайны;
>• средств и методов защиты коммерческой тайны;
>• проводимых мероприятий.
Сложность обеспечения защиты информации требует создания специальной службы, осуществляющей реализацию всех защитных мероприятий и в первую очередь организационного плана. Структура, численность и состав службы безопасности компании определяются реальными потребностями (степенью влияния утраты конфиденциальной информации на показатели работы).
Впрочем, безопасность предприятия и защита информации может быть реализована следующими тремя путями:
>• абонементное обслуживание силами специальных организаций;
>• создание собственной службы безопасности;
>• комбинированный вариант.
Рассмотрим все эти варианты более подробно.
В первом случае специализированное предприятие (организация), имеющее лицензию на соответствующие виды деятельности, на высоком профессиональном уровне проводит полный комплекс работ, связанный с организацией защиты и поддержание состояния защищенности на должном уровне. Поскольку для получения лицензии Гостехкомиссии при Президенте РФ или ФАПСИ (см. подраздел 2.2.1) требуются квалифицированные кадры, дорогостоящие аппаратные, программные и технические средства контроля, методики проведения работ, то лицензия — своеобразная гарантия качества защиты. Однако этот способ имеет два крупных недостатка:
>• услуги такого рода очень дороги (и не только у нас);
>• специалисты не могут постоянно находиться на объекте, следовательно при разовом «наезде» вполне вероятен пропуск факта вторжения.
Во втором случае в фирме создается своя служба безопасности, имеющая, например, следующую структуру (рис. 2.2.5). Она возглавляется


**Рис. 2.2.5. Примерная структура службы безопасности предприятия**

начальником, которому подчинены служба охраны, инспектор безопасности, консультант по безопасности и служба противопожарной охраны. Основными задачами службы безопасности предприятия являются:
>• обеспечение безопасности производственно-торговой деятельности, защита информации и сведений, являющихся коммерческой тайной;

>• организация работы по правовой, организационной и инженерно-технической (физической, аппаратной, программной и математической) защите коммерческой тайны;
>• организация специального делопроизводства, исключающего несанкционированное получение сведений, являющихся коммерческой тайной;
>• предотвращение необоснованного допуска и открытого доступа к сведениям и работам, составляющим коммерческую тайну;
>• выявление и локализация возможных каналов утечки конфиденциальной информации в процессе повседневной производственной деятельности и в экстремальных (авария, пожар и др.) ситуациях;
>• обеспечение режима безопасности при проведении таких видов деятельности, как различные встречи, переговоры, совещания, заседания и другие мероприятия, связанные с деловым сотрудничеством на национальном и международном уровне;
>• обеспечение охраны зданий, помещений, оборудования, продукции и технических средств обеспечения производственной деятельности;
.>• обеспечение личной безопасности руководства и ведущих сотрудников и специалистов;
>• оценка маркетинговых ситуаций при неправомерных действиях злоумышленников и конкурентов.
Для решения указанных задач служба безопасности предприятия должна выполнять следующие общие функции:
>• организовывать и обеспечивать пропускной и внутриобъектовый (при наличии зон ограниченного доступа) режим в зданиях и помещениях, устанавливать порядок несения службы охраны, контролировать соблюдение требований режима сотрудниками, смежниками, партнерами и посетителями;
>• руководить работами по правовому и организационному регулированию отношений по защите коммерческой тайны;
>• участвовать в разработке основополагающих документов с целью закрепления в них требований обеспечения безопасности и защиты коммерческой тайны, в частности Устава, Коллективного договора. Правил внутреннего трудового распорядка, соглашений, подрядов, должностных инструкций и обязанностей руководства, специалистов, рабочих и служащих;
>• разрабатывать и осуществлять совместно с другими подразделениями мероприятия по обеспечению работы с документами, содержащими сведения, являющиеся коммерческой тайной, при всех видах работ, организовывать и контролировать выполнение требований «Инструкции по защите коммерческой тайны»;
>• изучать все стороны производственной, коммерческой, финансовой и другой деятельности для выявления и закрытия возможных каналов утечки конфиденциальной информации, вести учет и анализ нарушений режима безопасности, накапливать и анализировать данные о злоумышленных устремлениях конкурентов и других организаций получить доступ к информации о деятельности предприятия или его клиентов, партнеров, смежников;
>• организовывать и проводить служебные расследования по фактам разглашения сведений, утрат документов и других нарушений режима безопасности предприятия;
>• разрабатывать, вести, обновлять и пополнять «Перечень сведений, составляющих коммерческую тайну» и другие нормативные акты, регламентирующие порядок обеспечения безопасности и защиты информации;
>• обеспечивать строгое выполнение требований нормативных документов по защите коммерческой тайны;
>• осуществлять руководство службами и подразделениями безопасности подведомственных предприятий, организаций, учреждений и других в части оговоренных в договорах и условиях по защите коммерческой тайны;

>• организовывать и регулярно проводить учебу сотрудников предприятия и службы безопасности по всем направлениям защиты коммерческой тайны, добиваясь, чтобы к защите коммерческих секретов был достигнут глубоко обоснованный подход;
>• вести учет сейфов, металлических шкафов, специальных хранилищ и других помещений, в которых разрешено постоянное или временное хранение конфиденциальных документов;
**>•** вести учет выделенных для конфиденциальной работы помещений, технических средств в них, обладающих потенциальными каналами утечки информации;
>• поддерживать контакты с правоохранительными органами и службами безопасности соседних предприятий в интересах изучения криминогенной обстановки в районе (зоне).
При наличии подобной службы безопасности процесс организации защиты информации, описанный в подразделе 2.2.1, проходит по следующим этапам.
**Первый этап** (анализ объекта защиты) состоит в определении, что нужно защищать.
Анализ проводится по следующим направлениям:
>• какая информация в первую очередь нуждается в защите;
>• наиболее важные элементы (критические) защищаемой информации;
>• определяется срок жизни критической информации (время, необходимое конкуренту для реализации добытой информации);
>• определяются ключевые элементы информации (индикаторы), отражающие характер охраняемых сведений;
>• классифицируются индикаторы по функциональным зонам предприятия (производственно-технологические процессы, система материально-технического обеспечения производства, подразделения, управления и т. д.).
**Второй этап** сводится к выявлению угроз:
>• определяется — кого может заинтересовать защищаемая информация;
>• оцениваются методы, используемые конкурентами для получения этой информации;
>• оцениваются вероятные каналы утечки информации;
>• разрабатывается система мероприятий по пресечению действий конкурента.
**Третий** — анализируется эффективность принятых и постоянно действующих подсистем обеспечения безопасности (физическая безопасность документации, надежность персонала, безопасность используемых для передачи конфиденциальной информации линий связи и т. д.).
**Четвертый** — определение необходимых мер защиты. На основании проведенных на первых трех этапах аналитических исследований определяются необходимые дополнительные меры и средства по обеспечению безопасности предприятия.
**Пятый** — рассматриваются руководителями фирмы (организации) представленные предложения по всем необходимым мерам безопасности и расчет их стоимости и эффективности.
**Шестой** — реализация дополнительных мер безопасности с учетом установленных приоритетов.
**Седьмой** — осуществление контроля и доведение до персонала фирмы реализуемых мер безопасности.
Преимущества создания собственной службы безопасности очевидны:
отлично зная объект, сотрудников, возможные угрозы, т. е. владея обстановкой, своя служба постоянно находится на объекте, поэтому всегда готова отразить всевозможные угрозы...
Главная проблема заключается в том, что на создание и поддержание ее должного уровня (подбор и обучение сотрудников, закупка техники, лидензирование...) необходимо затратить много времени и выделить

серьезные средства. Достаточно отметить, что только на приобретение минимума технических средств контроля защищенности с учетом всего многообразия средств промышленного шпионажа требуется единовременное выделение не менее 20 000 $. Однако одной аппаратуры недостаточно, так как необходимо и знание специальных методик оценки опасности различных каналов утечки информации. В качестве образца такого методического обеспечения в Приложении 1 приведены рекомендации по оценке защищенности конфиденциальной информации от ее утечки за счет побочных электромагнитных излучений.

Следует особо отметить, что даже при наличии финансовой возможности приобрести специальную аппаратуру и наличии методик все равно требуется участие группы консультантов из числа опытных специалистов как в области защиты информации, так и в тех областях, знания которых необходимы для проведения квалифицированного анализа.

Таким образом, наиболее действенным должен быть третий, комбинированный вариант, а именно совместная работа службы безопасности и специализированных предприятий по защите информации. В этом случае общими усилиями разрабатывается некий план по защите информации, основные моменты которого приведены ниже.

**План мероприятий по защите коммерческих секретов предприятия**

1. Определение целей плана по защите коммерческой тайны. Ими могут быть:

>• предотвращение кражи коммерческих секретов;

>• предотвращение разглашения коммерческих секретов сотрудниками или их утечки через технические каналы.

2. Анализ сведений, составляющих коммерческую тайну, для чего надо:

>• определить, какие сведения на предприятии (технологические и деловые) являются коммерческой тайной;

**>•** установить места их накопления и хранения;

>• оценить возможности по перекрытию каналов утечки;

>• проанализировать соотношение затрат на защиту и возможных потерь при утере информации, если использованы различные технологии, обеспечивающие защиту коммерческой тайны;

>• назначить сотрудников, персонально ответственных за каждый участок системы обеспечения безопасности.

3. Обеспечить реализацию деятельности системы по следующим направлениям:

>• контроль сооружений и оборудования предприятия (обеспечение безопасности производственных и конторских помещений, охрана фото- и иного копировального оборудования, контроль посещений предприятия и т. п.);

**>•** работа с персоналом предприятия, в том числе проведение бесед при приеме на работу; инструктаж вновь потупивших на работу по правилам и процедурам, принятым для защиты коммерческой тайны на предприятии; обучение сотрудников правилам сохранения коммерческих секретов; стимулирование соблюдения конфиденциальности;

беседы с увольняющимися;

>• организация работы с конфиденциальными документами (установление порядка и правил ведения делопроизводства, контроль за конфиденциальными документами, контроль за публикациями, контроль и учет технических носителей конфиденциальных сведений, рассекречивание и уничтожение конфиденциальных документов, охрана чужих секретов);

>• работа с конфиденциальной информацией, циркулирующей в технических средствах и системах, которые обеспечивают трудовую деятельность (создание системы предотвращения утечки информации через технические каналы);

>• работа с конфиденциальной информацией, накопленной в компьютерных

системах (создание системы защиты электронной информации от несанкционированного доступа к ней; обеспечение контроля за использованием ЭВМ);

>• защита коммерческой тайны предприятия в организационно-правовых документах, в процессе заключения контрактов и договоров с коллективом, сотрудниками, смежниками, поставщиками и т. д. Здесь важно четко определить круг лиц, имеющих отношение к этой работе.

После составления определяются те мероприятия плана, которые выполняются специализированной организацией (наличие квалифицированных специалистов в конкретной области, техническая и методическая оснащенность) и те из них, которые осуществляются силами и средствами собственной службы безопасности (знание оперативной обстановки, динамичность...). При такой работе достигаются оптимальные результаты с точки зрения финансовых затрат и качества защиты.

**2.2.3. Добровольная аттестация объектов информатизации по требованиям безопасности информации**

В настоящее время единственным способом юридически обосновать достаточность организационных и технических мероприятий по защите информации, а также компетентность собственной службы безопасности является добровольная аттестация (при защите сведений, составляющих государственную тайну аттестация объектов обязательна). При этом под аттестацией объектов информатизации будем понимать комплекс организационно-технических мероприятий, в результате которых посредством специального документа — «Аттестата соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных Гостехкомиссией России. Наличие на объекте информатизации действующего «Аттестата соответствия» дает право обработки информации с соответствующим уровнем конфиденциальности и на период времени, установленными в «Аттестате соответствия» (АС).

Однако до начала процедуры аттестации необходимо подготовить объект информатизации. Эта работа проводится в несколько этапов.

1. Определяется перечень помещений, предназначенных для обсуждения конфиденциальных вопросов, а так же автоматизированных систем, предназначенных для обработки, хранения, передачи важнейшей информации.

2.Определяется класс АС (см. п.2.1.3).

3.Заключается договор на проектирование объекта в защищенном исполнении с организацией на это уполномоченной (п. 5 Лицензии Гостехкомиссии России, Приложение № 3).

4.0существляется закупка сертифицированных средств защиты информации (Перечень в приложении № 8)

5. Осуществляется монтаж технических средств защиты информации, организацией на это уполномоченной (п.3 Лицензии Гостехкомиссии России, Приложение № 3).

6. Проводится подготовка (переподготовка) службы безопасности в учебных центрах (п.6 Лицензии Гостехкомиссии России, Приложение № 3).

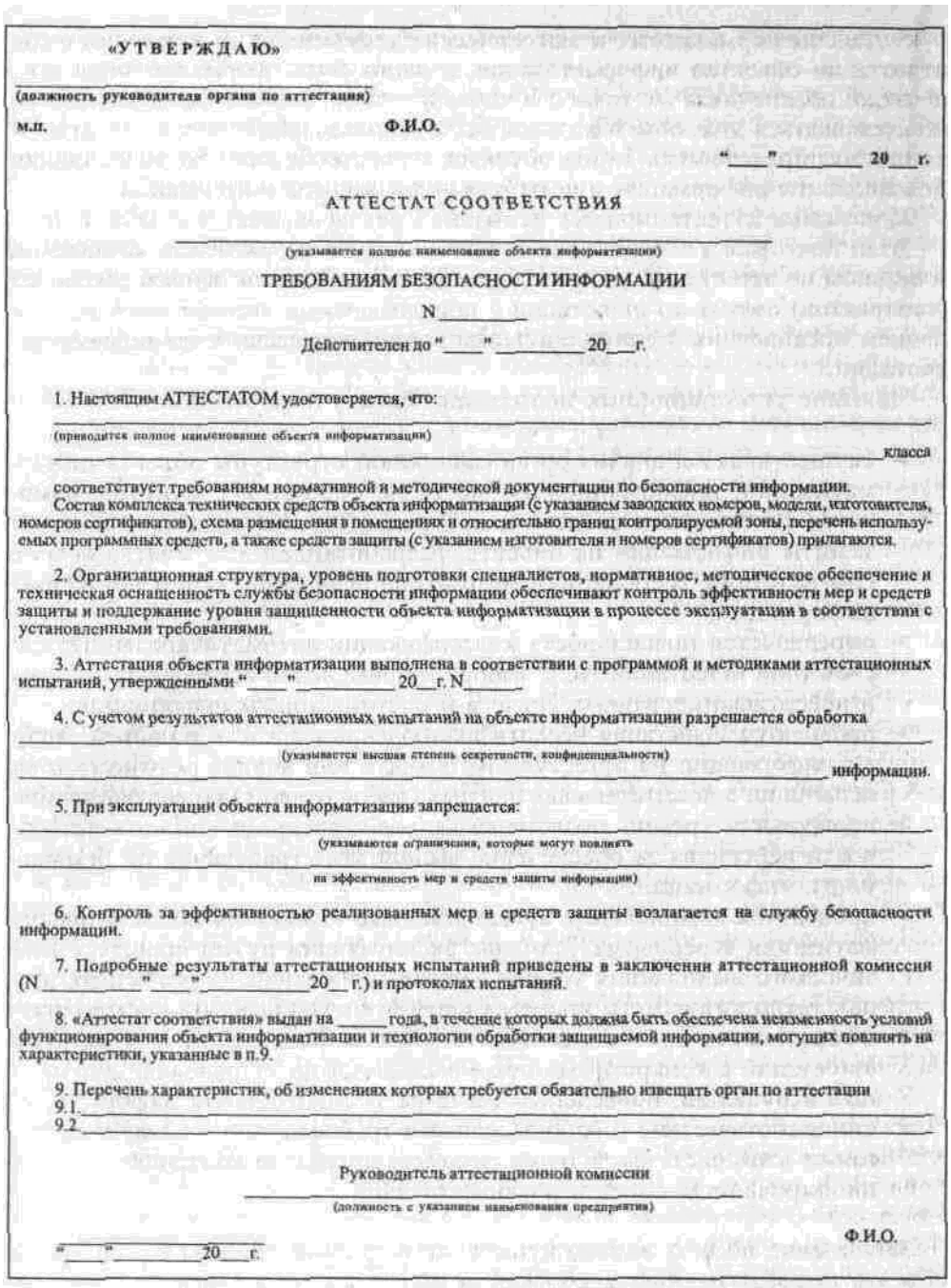
По окончанию этой работы возможно начинать аттестацию объектов. Основным руководящим документом является «Положение по аттестации объектов информатизации по требованиям безопасности информации», которое утверждено Председателем Государственной технической комиссии при Президенте Российской Федерации Ю. Яшиным 25 ноября 1994 г. Оно устанавливает основные принципы, организационную структуру системы аттестации объектов информатизации по требованиям безопасности информации, порядок проведения аттестации, а также контроля и надзора за аттестацией и эксплуатацией аттестованных объектов информатизации.

При аттестации объекта информатизации подтверждается его соответствие требованиям по защите информации от всех возможных угроз безопасности

информации, приведенных в ГОСТ «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (Приложение № 9).
Органы по аттестации аккредитуются Гостехкомиссией России в соответствии с «Положением об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации». Перечень органов по аттестации приведен в Приложении № 5.
Аттестация проводится в соответствии со схемой, выбираемой органом по аттестации на этапе подготовки к аттестации из следующего основного перечня работ:
>• анализ исходных данных по аттестуемому объекту информатизации;
>• предварительное ознакомление с аттестуемым объектом информатизации;
>• проведение экспертного обследования объекта информатизации и анализ разработанной документации по защите информации на этом объекте с точки зрения ее соответствия требованиям нормативной и методической документации;
>• проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств;
>• проведение испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации;
>• проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации;
>• анализ результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждение заключения по результатам аттестации.
Установлено, что органы по аттестации объектов информатизации несут ответственность за выполнение возложенных на них функций, обеспечение сохранности коммерческих секретов, а также за соблюдение авторских прав разработчиков аттестуемых объектов информатизации и их компонент.
Заявитель для получения «Аттестата соответствия» заблаговременно направляет в орган по аттестации заявку на проведение аттестации с исходными данными по аттестуемому объекту на основе следующего перечня вопросов:
1. Полного и точного наименования объекта информатизации и его назначение.
2. Характера (научно-техническая, экономическая, производственная, финансовая, политическая) и уровня конфиденциальности обрабатываемой информации.
3. Организационной структуры объекта информатизации.
4. Перечня помещений, состава комплекса технических средств (основных и вспомогательных), входящих в объект информатизации, в которых (на которых) обрабатывается указанная информация (расположенных в помещениях, где она циркулирует).
5. Особенности и схемы расположения объекта информатизации с указанием границ контролируемой зоны.
6. Структуры программного обеспечения (общесистемного и прикладного), используемого на аттестуемом объекте информатизации и предназначенного для обработки защищаемой информации, используемых протоколов обмена информацией.
7. Общей функциональной схемы объекта информатизации, включая схему информационных потоков и режимы обработки защищаемой информации.
8. Наличия и характера взаимодействия с другими объектами информатизации.
9. Состава и структуры системы защиты информации на аттестуемом объекте

информатизации.
10. Перечня технических и программных средств в защищенном исполнении, средств защиты и контроля, используемых на аттестуемом объекте информатизации и имеющих соответствующий сертификат, предписание на эксплуатацию (перечень сертифицированных средств защиты информации приведен в Приложении № 8).
11. Сведения о разработчиках системы защиты информации, наличие у сторонних разработчиков (по отношению к предприятию, на котором расположен аттестуемый объект информатизации) лицензий на проведение подобных работ (перечень лицензиантов приведен в Приложении № 3).
12. Наличия на объекте информатизации (на предприятии, на котором расположен объект информатизации) службы безопасности информации, службы администратора (автоматизированной системы, сети, баз данных).
13. Наличия и основных характеристик физической защиты объекта информатизации (помещений, где обрабатывается защищаемая информация и хранятся информационные носители).
14. Наличия и готовности проектной и эксплуатационной документации на объект информатизации и другие исходные данные по аттестуемому объекту информатизации, влияющие на безопасность информации.
Орган по аттестации рассматривает заявку и на основании анализа исходных данных выбирает схему аттестации, согласовывает ее с заявителем и принимает решение о проведении аттестации объекта информатизации.
При недостаточности исходных данных по аттестуемому объекту информатизации в схему аттестации включаются работы по предварительному ознакомлению с аттестуемым объектом, проводимые до этапа аттестационных испытаний.
При использовании на аттестуемом объекте информатизации несертифицированных средств и систем защиты информации в схему аттестации могут быть включены работы по их испытаниям в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации или непосредственно на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств. Перечень органов по сертификации приведен в Приложении № 6.
По результатам рассмотрения заявки и анализа исходных данных, а также предварительного ознакомления с аттестуемым объектом органом по аттестации разрабатываются программа аттестационных испытаний, предусматривающая перечень работ и их продолжительность, методики испытаний (или используются типовые методики), определяются количественный и профессиональней состав аттестационной комиссии, назначаемой органом по аттестации объектов информатизации, необходимость использования контрольной аппаратуры и тестовых средств на аттестуемом объекте информатизации или привлечения испытательных центров (лабораторий) по сертификации средств защиты информации по требованиям безопасности информации.
Порядок, содержание, условия и методы испытаний для оценки характеристик и показателей, проверяемых при аттестации, соответствия их установленным требованиям, а также применяемые в этих целях контрольная аппаратура и тестовые средства определяются в методиках испытаний различных видов объектов информатизации. При этом должны быть выполнены следующие условия.
1. Объекты информатизации, вне зависимости от используемых отечественных или зарубежных технических и программных средств, аттестуются на соответствие требованиям государственных стандартов или иных нормативных документов по безопасности информации, утвержденных Гостехкомиссией России.

2. Состав нормативной и методической документации для аттестации конкретных объектов информатизации определяется органом по аттестации в зависимости от вида и условий функционирования объектов информатизации на основании анализа исходных данных по аттестуемому объекту.
3. В нормативную документацию включаются только те показатели, характеристики, требования, которые могут быть объективно проверены.
4. В нормативной и методической документации на методы испытаний должны быть ссылки на условия, содержание и порядок проведения испытаний, используемые при испытаниях контрольную аппаратуру и тестовые средства, сводящие к минимуму погрешности результатов испытаний и позволяющие воспроизвести эти результаты.
5. Тексты нормативных и методических документов, используемых при аттестации объектов информатизации, должны быть сформулированы ясно и четко, обеспечивая их точное и единообразное толкование. В них должно содержаться указание о возможности использования документа для аттестации определенных типов объектов информатизации по требованиям безопасности информации или направлений защиты информации.
Программа аттестационных испытаний согласовывается с заявителем.
Этап подготовки завершается заключением договора между заявителем и органом по аттестации на проведение аттестации, заключением договоров (контрактов) органа по аттестации с привлекаемыми экспертами и оформлением предписания о допуске аттестационной комиссии к проведению аттестации.
На этапе аттестационных испытаний объекта информатизации:
>• осуществляется анализ организационной структуры объекта информатизации, информационных потоков, состава и структуры комплекса технических средств и программного обеспечения, системы защиты информации на объекте, разработанной документации и ее соответствия требованиям нормативной документации по защите информации;
>• определяется правильность классификации автоматизированных систем (при аттестации АС), выбора и применения сертифицированных и несертифицированных средств и систем защиты информации;
>• проводятся испытания несертифицированных средств и систем защиты информации на аттестуемом объекте или анализ результатов их испытаний в испытательных центрах (лабораториях) по сертификации;
**>•** проверяется уровень подготовки кадров и распределение ответственности персонала за обеспечение выполнения требований по безопасности информации;
**>•** проводятся комплексные аттестационные испытания объекта информатизации в реальных условиях эксплуатации путем проверки фактического выполнения установленных требований на различных этапах технологического процесса обработки защищаемой информации;
>• оформляются протоколы испытаний и заключение по результатам аттестации с конкретными рекомендациями по устранению допущенных нарушений, приведению системы защиты объекта информатизации в соответствие с установленными требованиями и совершенствованию этой системы, а также рекомендациями по контролю за функционированием объекта информатизации.
Заключение по результатам аттестации с краткой оценкой соответствия объекта информатизации требованиям по безопасности информации, выводом о возможности выдачи «Аттестата соответствия» и необходимыми



«УТВЕРЖДАЮ»

_____

(должность руководителя органа по аттестации)

м.п. Ф.И.О.

"____"_____ 20___г.

АТТЕСТАТ СООТВЕТСТВИЯ

_____

(указывается полное наименование объекта информатизации)

ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

N_____

Действителен до "____"_____20___г.

1. Настоящим АТТЕСТАТОМ удостоверяется, что:

_____

(приводится полное наименование объекта информатизации)

_____класса

соответствует требованиям нормативной и методической документации по безопасности информации.

Состав комплекса технических средств объекта информатизации (с указанием заводских номеров, модели, изготовителя, номеров сертификатов), схема размещения в помещениях и относительно границ контролируемой зоны, перечень используемых программных средств, а также средств защиты (с указанием изготовителя и номеров сертификатов) прилагаются.

2. Организационная структура, уровень подготовки специалистов, нормативное, методическое обеспечение и техническая оснащенность службы безопасности информации обеспечивают контроль эффективности мер и средств защиты и поддержание уровня защищенности объекта информатизации в процессе эксплуатации в соответствии с установленными требованиями.

3. Аттестация объекта информатизации выполнена в соответствии с программой и методиками аттестационных испытаний, утвержденными "____"_____20___г. N_____

4. С учетом результатов аттестационных испытаний на объекте информатизации разрешается обработка

_____

(указывается высшая степень секретности, конфиденциальности)

_____информации.

5. При эксплуатации объекта информатизации запрещается:

_____

(указываются ограничения, которые могут повлиять

_____

на эффективность мер и средств защиты информации)

6. Контроль за эффективностью реализованных мер и средств защиты возлагается на службу безопасности информации.

7. Подробные результаты аттестационных испытаний приведены в заключении аттестационной комиссии (N _____"____"_____20___г.) и протоколах испытаний.

8. «Аттестат соответствия» выдан на _____года, в течение которых должна быть обеспечена неизменность условий функционирования объекта информатизации и технологии обработки защищаемой информации, могущих повлиять на характеристики, указанные в п.9.

9. Перечень характеристик, об изменениях которых требуется обязательно извещать орган по аттестации

9.1._____

9.2._____

Руководитель аттестационной комиссии

_____

(должность с указанием наименования предприятия)

Ф.И.О.

"____"_____20___г.

**Рис. 2.2.6. Форма «Аттестата соответствия требованиям безопасности»**

рекомендациями подписывается членами аттестационной комиссии и доводится до сведения заявителя. К заключению прилагаются протоколы испытаний, подтверждающие полученные при испытаниях результаты и обосновывающие приведенный в заключении вывод. Протоколы испытаний подписываются экспертами — членами аттестационной комиссии, проводившими испытания. Заключение и протоколы испытаний подлежат утверждению органом по аттестации.

«Аттестат соответствия» оформляется и выдается заявителю после утверждения заключения по результатам аттестации по форме представленной на рис 2.2.6.

«Аттестат соответствия» выдается владельцу аттестованного объекта

информатизации органом по аттестации на период, в течение которого обеспечивается неизменность условий функционирования объекта информатизации и технологии обработки защищаемой информации, могущих повлиять на характеристики, определяющие безопасность информации (состав и структура технических средств, условия размещения, используемое программное обеспечение, режимы обработки информации, средства и меры защиты), но не более, чем на 3 года. Владелец аттестованного объекта информатизации несет ответственность за выполнение установленных условий функционирования объекта информатизации, технологии обработки защищаемой информации и требований по безопасности информации.

В случае изменения условий и технологии обработки защищаемой информации владельцы аттестованных объектов обязаны известить об этом орган по аттестации, который принимает решение о необходимости проведения дополнительной проверки эффективности системы защиты объекта информатизации.

При несоответствии аттестуемого объекта требованиям по безопасности информации и невозможности оперативно устранить отмеченные аттестационной комиссией недостатки орган по аттестации принимает решение об отказе в выдаче «Аттестата соответствия». При этом может быть предложен срок повторной аттестации при условии устранения недостатков. При наличии замечаний непринципиального характера «Аттестат соответствия» может быть выдан после проверки устранения этих замечаний.

В случае несогласия заявителя с отказом в выдаче «Аттестата соответствия» он имеет право обратиться в вышестоящий орган по аттестации или непосредственно в Гостехкомиссию России с апелляцией для дополнительного рассмотрения полученных при испытаниях результатов, где она в месячный срок рассматривается с привлечением заинтересованных сторон. Податель апелляции извещается о принятом решении.

## 2.3. Методы и средства выявления закладных устройств

### 2.3.1. Общие принципы выявления

Одним из элементов системы защиты информации является выявление возможно внедренных закладных устройств (ЗУ). Оно реализуется на основе двух групп методов (рис. 2.3.1).


**Рис. 2.3.1. Методы выявления закладных устройств**

Первая группа — методы, основанные на поиске ЗУ как физических объектов с вполне определенными свойствами и массогабаритными характеристиками. К ней относятся:

>• визуальный осмотр мест возможного размещения ЗУ, в том числе с применением увеличительных стекол, зеркал, средств специальной подсветки;

**>•** контроль труднодоступных мест с помощью средств видеонаблюдения;

>• применение металлодетекторов.

Вторая группа — методы, использующие свойства ЗУ как электронных систем. Она включает:

>• использование индикаторов поля, реагирующих на наличие излучения радиозакладных устройств и позволяющих локализовать их месторасположение;

>• применение специальных радиоприемных устройств, предназначенных для поиска сигналов по заданным характеристикам и анализа электромагнитной обстановки;

**>•** применение комплексов радиоконтроля и выявления ЗУ;

>• обследование помещений с помощью нелинейных радиолокаторов, позволяющих выявлять любые типы ЗУ (см. п. 1.3, 1.4).

Обнаружение ЗУ как физических объектов является наиболее общим случаем, попадающим под понятие осмотра или досмотра. Его основные методы и

используемые технические средства будут рассмотрены в п. 2.3.1. Каждому из методов второй группы будет посвящен отдельный подраздел.

**Методы поиска закладных устройств как физических объектов**

**Визуальный осмотр**

Это один из важнейших методов выявления, он не может быть заменен ни одним другим. Он предназначен для обнаружения ЗУ как в обычном исполнении, так и в закамуфлированном виде. Осуществляется периодически, а также перед проведением важных мероприятий в тех помещениях, где возможно размещение ЗУ.

При проведении визуального осмотра особое внимание обращается на изменения в интерьере, появление свежих царапин, следов подчистки или подкраски. Особенно тщательно осматриваются (с полной или частичной разборкой) сувениры, забытые посетителями личные вещи или другие «случайные» предметы. Проводится обязательный осмотр телефонных и других линий связи на участке от аппарата до распределительной коробки.

При проведении осмотра особое внимание уделяется скрытым и труднодоступным местам, так как именно они представляют наибольший интерес для лиц, устанавливающих ЗУ. Для облегчения процедуры поиска используют фонари и зеркала (рис. 2.3.2).

Однако такие простые приспособления не всегда удобны и эффективны, поэтому на практике зачастую применяют технические средства видеонаблюдения, специально приспособленные для осмотра труднодоступных мест.

Контроль с помощью средств видеонаблюдения

К современным средствам видеонаблюдения относят оптико-электронные системы, которые условно можно разбить на две группы:

>• эндоскопическое оборудование;

>• досмотровые портативные телевизионные или видеоустановки.


**Рис. 2.3.2. Средства для проведения осмотра в труднодоступных местах:**
а — фонари Mag-Lite (оборудованы устройством, позволяющим изменять световой пучок от точечного до рассеянного); о — специальные зеркала, предназначенные для проведения осмотра в труднодоступных местах

Ассортимент **эндоскопической продукции** включает в себя целую гамму волоконно-оптических фиброскопов, жесткие бароскопов, а также видеоскопов, позволяющих осуществлять осмотр труднодоступных мест.

Отличительной особенностью этих устройств является миниатюрный объектив, помещенный на конце тонкого гибкого рукава или жесткой трубки, которые служат и направляющим элементом, и защитной оболочкой для оптоволоконного жгута (реже многокомпонентной линзовой системы), предназначенного для передачи изображения с выхода объектива на окуляр либо ПЗС-матрицу. В некоторых типах видеоскопов ПЗС-матрица расположена непосредственно на зондирующем конце рукава или трубки. С выхода матрицы сигнал по кабелю или радиоканалу передается в блок преобразования и далее на монитор.

Гибкие фиброскопы предназначены для проникновения сквозь сложные изгибы различных каналов (рис. 2.3.3, а, б). Бароскопы используются для осмотра узлов, к которым может быть осуществлен доступ через узкие прямолинейные каналы. В отличие от фиброскопов, вместо гибкого рукава они оборудованы жесткой штангой (рис. 2.3.3, в). Особенностью видеоскопов является то, что они позволяют в реальном масштабе времени осуществлять вывод изображения на телевизионный монитор, с одновременным фото- и (или) видеодокументированием, как, например, устройство РК 1700 (рис. 1.4.13, з). Кроме того, видеоскопы позволяют вести наблюдение за объектами, находящимися на удалении до 22 м.

Общим недостатком эндоскопических устройств является то обстоятельство, что они, скорее, рассчитаны на статическое скрупулезное обследование, чем на быстрый оперативный осмотр. Кроме того, зачастую эти системы имеют многомодульную конфигурацию с кабельными соединениями, их функциональные блоки не минимизированы по весу и габаритам (РК 1765, РК 1700). Очевидны и проблемы с быстрой подготовкой к работе, переносом системы и сохранением ее целостности. Еще одна существенная особенность заключается в не всегда приемлемом качестве наблюдаемого через окуляр изображения.

Сравнительная оценка эндоскопических устройств различного типа показывает, что наилучшее качество изображения позволяют получать видеоскопы, кроме того, по телевизионному монитору следить за осмотром может практически неограниченное число наблюдателей. В то же время, подобное оборудование не может использоваться одним оператором и не приспособлено для быстрой смены места осмотра и обхода объектов. Для этих целей больше подходят портативные эндоскопические устройства типа фиброскопов МР-660В, ММ-013С или РК 1760.

**Досмотровые портативные телевизионные системы** позволяют соединить достоинства высокого качества изображения с максимальным удобством пользования оборудованием при осмотре. Это достигается путем конструктивного объединения в едином устройстве миниатюрной телевизионной камеры, регулируемой штанги и телевизионного монитора.

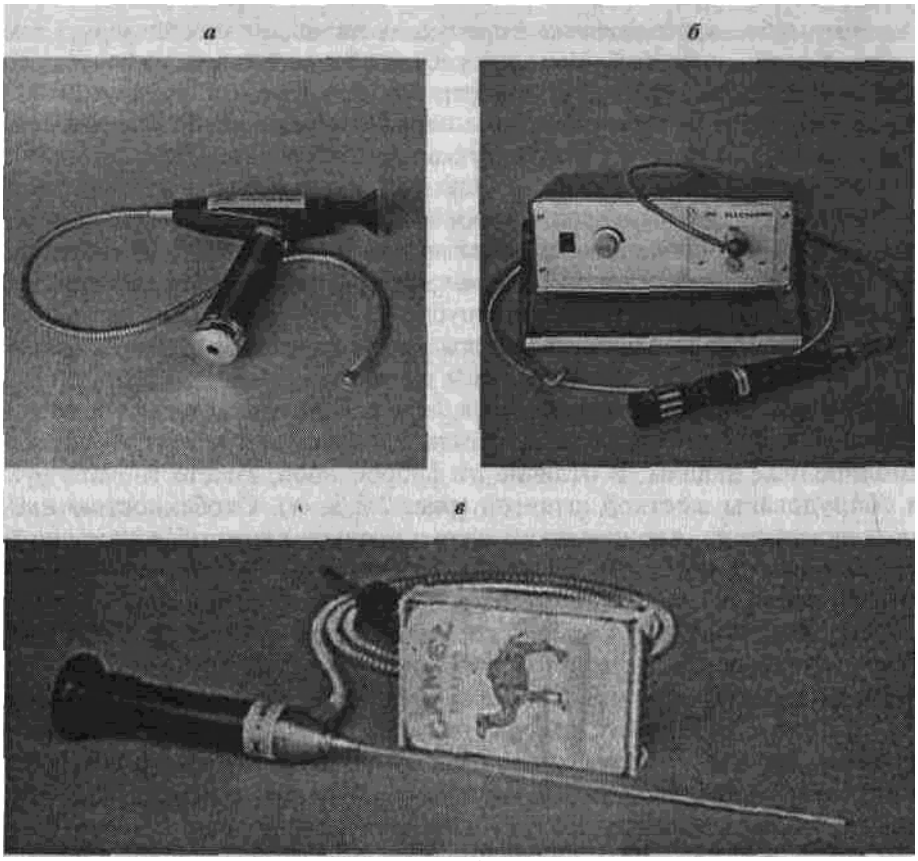



**Рис. 2.3.3. Эндоскопическое оборудование:**
а — фиброскоп РК 1760; б — фиброскоп РК 1765; в — бароскоп РК 1700-S

Такое оборудование специально разрабатывается для нужд таможенных служб, но достаточно эффективно может быть использовано и для поиска ЗУ.

В качестве примера можно привести носимое досмотровое видеоустройство Альфа-4 (рис. 2.3.4), в комплект которого входят следующие основные компоненты:

>• телескопическая штанга с черно-белой видеокамерой и источником инфракрасной подсветки, позволяющие досматривать объекты на удалении до 2,5 м;

**>•** миниатюрный жидкокристаллический видеомонитор, размещаемый в руке оператора;

**>•** специальный жилет, носимый поверх одежды.

**Рис. 2.3.4. Носимое досмотровое видеоустройство Альфа-4:**
а — поиск «бамперных жучков» с использованием носимого оборудования;
б — стационарная приемная телевизионная станция
В жилете размещены пульт управления и индикации, миниатюрный микрофон, аккумуляторный блок питания и передатчик телевизионного сигнала с антенной. Последний используется в том случае, если необходима трансляция изображения на стационарную телевизионную станцию для более тщательного контроля и документирования.
Другим примером реализации портативной телевизионной аппаратуры досмотра может служить система S-1000 («Кальмар»), имеющая аналогичную комплектацию. Ее характерными особенностями являются следующие:
>• изделие оборудовано пылевлагозащитным и ударопрочным корпусом, предохраняющим устройство от влияния окружающей среды, а герметизация камеры позволяет осуществлять осмотр даже в жидких средах;
**>•** цилиндрический корпус камеры со встроенной инфракрасной подсветкой обеспечивает максимально возможную для этого оборудования способность проникновения в труднодоступные места;
>• угловое положение камеры изменяется с помощью гибкой концевой штанги или фиксируемого шарнира;
>• телевизионный сигнал и питание передаются по кабелю, пропущенному внутри телескопической штанги. Здесь же обеспечивается автоматическая подмотка избыточного кабеля на встроенный подпружиненный барабан;
>• компактный монитор с электронно-лучевой трубкой крепится на штанге с помощью регулируемого кронштейна.

**Применение металлодетекторов**

Недостатком визуального осмотра является необходимость длительной повышенной концентрации внимания оператора, что не всегда дает надежный результат. Поэтому следующий шаг в повышении эффективности выявления ЗУ связан с объединением возможностей визуального и детекторного исследований.
Под детекторным исследованием понимается применение аппаратуры, которая контактным или бесконтактным способом воспринимает определенные физические свойства, свидетельствующие о наличии в обследуемом месте некоторых аномалий в виде неоднородностей, характерных излучений или конкретных веществ. С точки зрения эффективности обследования с применением детекторов существенно то, что они вырабатывают звуковой или световой сигнал в случае превышения заданного порога параметром, по которому осуществляется детектирование. Тем самым происходит не только выявление, но и локализация искомого устройства или предмета. Все в дальнейшем рассматриваемые методы являются детекторными.
Металлоискатели являются наиболее простым типом детекторов ЗУ, действующим по принципу выявления металлических предметов (элементов ЗУ) в непроводящих и слабопроводящих средах (дерево, одежда, пластмасса и т. п.). Детекторы бывают как ручного, так и арочного типа. Естественно, что для вышеопределенных целей подходят только ручные приборы. В настоящее время известны сотни модификаций металлодетекторов. Однако по принципу работы они почти яе отличаются друг от друга, а их основные особенности составляют только потребительские и эксплуатационные характеристики.
Практически все современные металлоискатели предназначены для поиска предметов как из черных, так и из цветных металлов. При этом обнаружительная способность по дальности лежит в пределах от 10 до 500 мм и зависит, главньм образом, от массы предмета. Все приборы имеют звуковую, а иногда и световую сигнализацию.
Приведем следующие типы металлодетекторов (рис. 2.3.5).
**АКА 7202М** — селективный металлодетектор, предназначенный для поиска металлических предметов в диэлектрических и слабопроводящих средах.

Подает различные звуковые сигналы при приближении к предметам из черных и цветных металлов. Максимальная дальность обнаружения: 80 мм — винт М3х7; 100 мм — диск 15х1 мм. Питание — «Крона» 9 В.

**МАРС** — металлодетектор, предназначенный для оперативного поиска предметов из черных и цветных металлов. Питание — «Крона» 9 В.

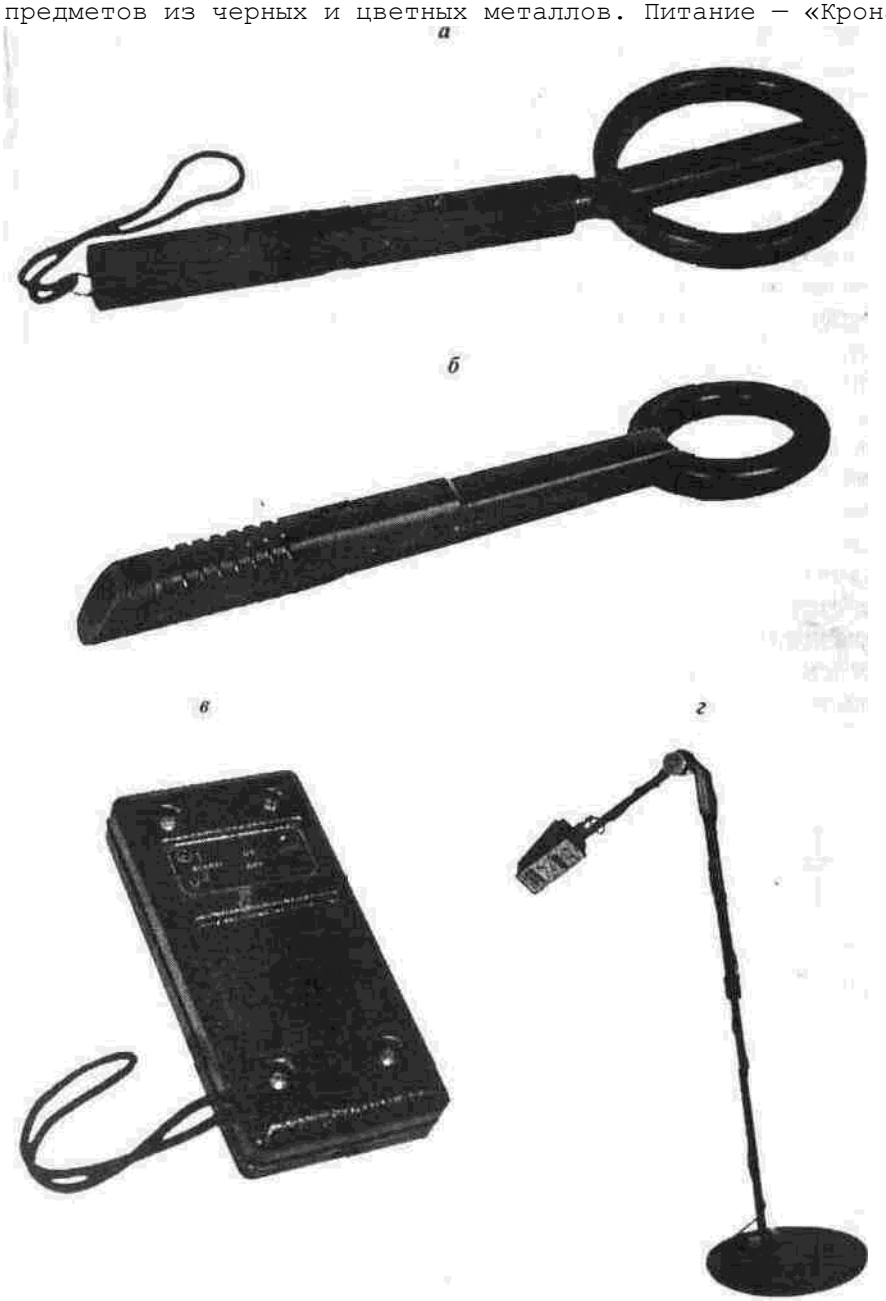



**Рис. 2.3.5. Металлодетекторы:**
а — АКА 7202М; б — МАРС; в - МИНИСКАН; г — СТЕРХ-92АР

**МИНИСКАН** — малогабаритный селективный металлодетектор, предназначенный для оперативного обнаружения металлических предметов. Подает различные звуковые сигналы при приближении к предметам из черных и цветных металлов. Не нуждается в предварительных настройках. Питание — «Крона» 9 В.

**СТЕРХ-92АР** — металлодетектор, предназначенный для поиска металлических предметов в диэлектрических и слабопроводящих средах. Максимальная

дальность обнаружения металлических предметов: 250 мм — диск 20х1 мм; 600 мм — пластина 100х100х1 мм. Питание — «Крона» 9 В.

Простейший металлодетектор, работающий на принципе сравнения двух частот, представлен на рис.2.3.5, д.

Одна из частот является эталонной, другая изменяется при попадании металлических предметов в поле действия чувствительного элемента (поисковой катушки).

Для повышения чувствительности устройства частоты генераторов выбраны отличающимися на порядок. Так, эталонный генератор выполнен на двух логических элементах DD2, частота его стабилизирована кварцевым резонатором ZQ1 (1 МГц). Генератор же с изменяющейся частотой выполнен на первых двух элементах DD1, его колебательный контур об-

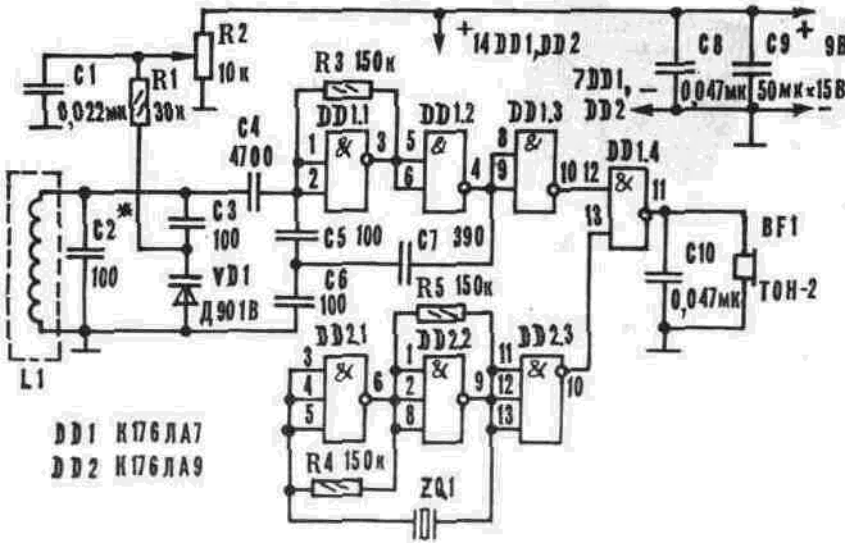



**Рис. 2.3.5, д. Принципиальная электрическая схема металлодетектора**

разовая поисковой катушкой L1, конденсаторами С2 и С3, а также варикапом VD1. Для настройки на заданную частоту (100 кГц) генератор 2 содержит резистор R2, создающий требуемое напряжение на варикапе VD1.

Особой тщательности при изготовлении металлодетектора требует выполнение поисковой катушки. Наматывается она на виниловой трубке с внешним диаметром 15 мм и внутренним — 10 мм, согнутой в форме окружности Ж 200 мм. Катушка содержит 100 витков провода ПЭВ-0,27, закрытых сверху электростатическим экраном из металлической фольги. Для защиты самого экрана от внешних механических воздействий применяется изоляционная бандажная лента.

Подготовка прибора к работе заключается в настройке его чувствительности на уровень фона потенциометром R2, тогда любой металлический предмет, попавший в поле поисковой катушки будет вызывать возникновение звукового сигнала в головном телефоне BF1.

### 2.3.2. Индикаторы поля

В соответствии с классификацией, приведенной на рис. 2.3.1, основными способами выявления радиозакладных устройств являются:

- использование индикаторов поля;
- применение специальных приемников;
- применение комплексов радиоконтроля.

Все они основаны на наличии у данного типа ЗУ радиоизлучений, которые кроме того, что сами по себе являются демаскирующим признаком, обладают еще и рядом характерных особенностей, позволяющих идентифицировать их именно как сигналы радиозакладок. Поэтому, с точки зрения поиска, радиозакладное устройство — очень удобный объект. Отметим эти особенности.

**Основные признаки излучения радиозакладок**

**Первый** признак — относительно высокий уровень излучения, обусловленный необходимостью передачи сигнала за пределы контролируемого помещения. Этот уровень тем выше, чем ближе к ЗУ находится аппаратура поиска.

**Второй** — наличие гармоник в излучении радиозакладок. Это обстоятельство является следствием необходимости минимизации размеров ЗУ, а следовательно невозможности обеспечить хорошую фильтрацию выходного излучения. В современных радиозакладках ослабление излучений на гармониках составляет всего 40—50 дБ, поэтому обнаружение этих нежелательных излучений без особых проблем возможно на удалении до 10 м, естественно, если позволяет частотный диапазон применяемого приемника контроля.

**Третий** — появление нового источника в обычно свободном частотном диапазоне. При этом оператор, осуществляющий радиоконтроль, должен очень хорошо ориентироваться в общей радиоэлектронной обстановке и знать, что и в каких диапазонах может работать.

**Четвертый** связан с использованием в ряде радиозакладок направленных антенн. Это приводит к сильной локализации излучения, то есть существенной неравномерности его уровня в пределах контролируемого объекта. На расстояниях в несколько метров этот эффект лучше всего проявляется для гармоник основного излучения.

**Пятый** признак связан с особенностями поляризации излучения радиозакладок. Дело в том, что при изменении пространственного положения или ориентации приемной антенны наблюдается изменение уровня всех источников. Однако однотипные удаленные источники одного диапазона ведут себя примерно одинаково, тогда как сигнал закладки изменяется отлично от остальных. На практике этот эффект наверняка замечали те, кто осуществлял поиск ЗУ с использованием анализаторов спектра.

**Шестой** признак заключается в изменении («размывании») спектра излучений радиомикрофонов при возникновении каких-либо шумов в контролируемом помещении. Он проявляется только в том случае, если ЗУ работает без кодирования передаваемой информации.

**Седьмой** признак связан со способностью человека различать акустические сигналы. Так, если закладка работает без маскирования, то оператор, осуществляющий поиск ЗУ, слышит шум помещения или тот тестовый сигнал, который сам создал. В аппаратном варианте этот эффект обыгрывается разного рода корреляторами и так называемой акустической завязкой. При выявлении закладок с маскированием передаваемой информации сигнал напоминает неразборчивую речь или какофонию, если в качестве тестовых используются, соответственно, речевой сигнал или музыка. В последнем случае для аппаратного выявления необходимы специальные алгоритмы корреляции, но обычно можно обойтись и просто зондированием импульсными акустическими сигналами. Наконец, при применении кодирования, скорее всего, оператор будет слышать белый шум, и, скорее всего, никакая корреляция со звуком в данном случае не поможет.

**Восьмой** признак связан со временем работы радиозакладок. Так, самые простые из них, то есть не оборудованные схемами дистанционного включения и VOX, будут функционировать непрерывно в течение некоторого времени. Для закладок с VOX характерен прерывистый режим работы днем и практически полное молчание ночью. Устройства с дистанционным включением обязательно имеют несколько коротких сеансов в течение дня и почти наверняка будут работать во время переговоров, важных с точки зрения установившего их лица. Применительно к телефонным закладкам наличие восьмого признака проверяется очень просто: если какое-либо излучение возникает одновременно с поднятием трубки и исчезает, когда трубка положена, то это излучение прямо или косвенно связано с утечкой информации.

Вышеприведенный список признаков не является исчерпывающим и может быть существенно расширен. Более подробная информация о процедуре поиска ЗУ приведена в п. 2.3.6.

**Применение индикаторов (детекторов) поля**

Простейшими средствами обнаружения факта использования радиозакладок являются индикаторы, или детекторы поля. По сути, это приемники с очень низкой чувствительностью, поэтому они обнаруживают излучения радиозакладных устройств на предельно малых расстояниях (10—40 см), чем и обеспечивается селекция нелегальных излучений на фоне мощных разрешенных сигналов. Важное достоинство детекторов — способность находить передающие устройства вне зависимости от применяемой в них модуляции. Основной принцип поиска состоит в выявлении абсолютного максимума уровня излучения в помещении. Хорошие индикаторы поля снабжены частотомерами, акустическими динамиками, имеют режим прослушивания и двойную индикацию уровня сигнала.

Иногда детекторы используют и в так называемом сторожевом режиме. В этом случае после полной проверки помещения на отсутствие ЗУ фиксируется уровень поля в некоторой точке пространства (обычно это стол руководителя или место ведения переговоров), и прибор переводится в дежурный режим. В случае включения закладки (примерно на удалении до двух метров от детектора) индикатор выдает сигнал о повышении уровня электромагнитного поля. Однако необходимо учитывать тот факт, что если будет использоваться радиозакладка с очень низким уровнем излучения, то детектор скорее всего не зафиксирует ее активизацию.

В некоторых случаях (при наличии достаточного времени) можно даже составить карту помещения, зафиксировав характерные уровни излучения в каждой точке пространства. Для достижения данной цели особенно удобны детекторы, снабженные цифровой индикацией уровня, например такие, как новая разработка фирмы Optoelectronics RF Detector или отечественный «Энтомолог-5».

Так как индикаторы поля должны реагировать на уровень электромагнитного излучения, то в них применяют амплитудные детекторы, которые дают дополнительный эффект, позволяющий прослушивать сигналы от радиозакладок с амплитудной модуляцией. Однако в ряде случаев наблюдается и детектирование излучений радиомикрофонов с частотной модуляцией. Это происходит как за счет неравномерности амплитудно-частотной характеристики индикатора, так и за счет неизбежной паразитной амплитудной модуляции, характерной для большинства закладок. Поскольку для индикатора частотная демодуляция — побочный эффект, то уровень демодулированного сигнала обычно невелик. Наличие же закладки обращает на себя внимание общим понижением уровня фона, создаваемого телевидением и вещательными станциями. Хорошие результаты по обнаружению дает также шум, возникающий при трении куска мягкого пенопласта по обследуемой поверхности.

Если индикатор снабжен частотомером, то это позволяет реализовать еще одну возможность. Дело в том, что в некоторых приборах частотомер имеет фиксированный порог и в этом случае его срабатывание и отсчет одной и той же частоты в последовательных измерениях серьезный признак высокого уровня сигнала и, следовательно, наличия закладки. В других индикаторах частотомер работает при любом уровне сигнала и на него следует обращать внимание только тогда, когда он показывает одну и ту же частоту.

Примером индикаторов, в том числе и индикаторов-частотомеров, применяемых для обнаружения радиозакладок, могут служить следующие устройства.

**Cub** — прибор, предназначенный для измерения частоты радиосигналов и [1] поиска подслушивающих устройств. Он имеет цифровой фильтр, функцию автозахвата, девятизначный дисплей. Его рабочий диапазон 1...2,8 МГц,

чувствительность в зависимости от поддиапазона колеблется от 300 мкВ до 25 мВ. Период проведения измерений регулируется от 0,0001 до 0,64 с.

**Optoelectronics Ml** — предназначен для измерения частот радиосигналов, а также для обнаружения и локализации радиопередатчиков, работающих в двух поддиапазонах:10 Гц...50 МГц и 200 МГц...2,8 ГГц. Чувствительность 3—50 мВ. Имеется встроенный микроконтроллер, который обеспечивает цифровую фильтрацию, цифровой автозахват, сохранение и последовательный вывод данных. Подключение к приемнику конвертора модели CX 12RS-232 позволяет протоколировать данные на персональном компьютере. Прибор имеет десятиразрядный жидкокристаллический дисплей, его габариты — 125x70x35 мм. Питание осуществляется от встроенного ni-cd аккумулятора с напряжением 9 В, которого хватает на 4—5 ч непрерывной работы.

**Scout-40** — устройство, предназначенное для измерения частот радиосигналов с интервалом 10 мс, а также обнаружения и локализации радиопередатчиков в диапазоне частот 10 МГц...1,4 ГТд. Для уменьшения ложных отсчетов изделие осуществляет цифровую фильтрацию и проверку приходящих сигналов на стабильность и когерентность. Scout позволяет запоминать до 400 различных частот, а также отмечать до 255 периодов активности на каждой из них. Встроенный интерфейс Optoscan 456 позволяет использовать частотомер для управления приемниками (ICOM R7000, R7100, R9000, AOR AR2700, AR8000 и др.). Чувствительность приемника около 1 мВ. Десятиразрядный жидкокристаллический дисплей; питание от встроенного ni-cd аккумулятора (6 В), обеспечивающего 10 ч непрерывной работы. Габариты — 94x70x30 мм.

**MRA-3** — автоматический приемник ближней зоны. Предназначен для повседневного контроля радиообстановки и выявления вновь появляющихся радиосигналов, в том числе от устройств несанкционированного съема информации с дистанционным управлением.

В автоматическом режиме обеспечивает запоминание спектра сигналов с возможностью дополнения его новыми известными частотами, регистрацию и запоминание новых сигналов с выдачей сигнала тревоги.

Его основные технические характеристики: диапазон рабочих частот 42... 2700 МГц; виды модуляции принимаемых сигналов WFM, NFM, AM; время сканирования диапазона — 6с; количество запоминаемых в фоновом режиме частот — 512; число новых запоминаемых новых сигналов — 16; индикация — звуковая, жидкокристаллический дисплей, светодиодная; питание от аккумулятора 9 В или сетевого адаптера. Габариты 136x49x137 мм.

**ПИТОН** — приемник-детектор, предназначенный для обнаружения и демодуляции частотномодулированных сигналов, используемых в вещательных радиопередатчиках, а также поиска несанкционированных радиопередатчиков с использованием акустозавязки и индикатора уровня принимаемого сигнала.

Технические характеристики прибора: диапазон частот — от 30... 1000 МГц; чувствительность не хуже — 48 дБ относительно 1 В; время сканирования диапазона не более 2 с; задержка поиска после пропадания сигнала — не более 3 с; питание от 6 элементов по 1,5 В. Габариты — 146x70x45 мм.

**R-11** — тестовый приемник для работы в ближней зоне, анализирующий гармоники основных частот радиоизлучений для поиска радиозакладок. Диапазон его рабочих частот лежит в интервале от 30 МГц до 2 ГГц. Время поиска по диапазону не превышает 1 с. Чувствительность около 100 мВ.

К сожалению, использование индикатора поля в качестве единственного поискового прибора весьма неудобно, так как связано с необходимостью обследования всех возможных мест размещения закладки на расстояниях не менее 10 см (при дальностях порядка 40 см вероятность пропуска закладки может составить уже десятки процентов).

Не следует особенно полагаться и на широко рекламируемую функцию

акустической завязки (например, приемник **ПИТОН).** Дело в том, что этот эффект связан с необходимостью возникновения положительной обратной связи в цепи «собственный динамик с тестовым сигналом — радиомикрофон — приемник индикатора поля». А для формирования такой связи требуется выполнение определенных фазовых соотношений для звуковой волны, достаточно высокий уровень звукового сигнала и время установления не менее 1—2 с. Поэтому для гарантированного возникновения эффекта завязки на расстоянии от полуметра необходимо максимально повысить уровень звука на индикаторе и перемещать детектор в пространстве максимально медленно.

Обобщенные технические характеристики наиболее распространенных детекторов поля приведены в табл. 2.3.1, а внешний вид на рис. 2.3.6.

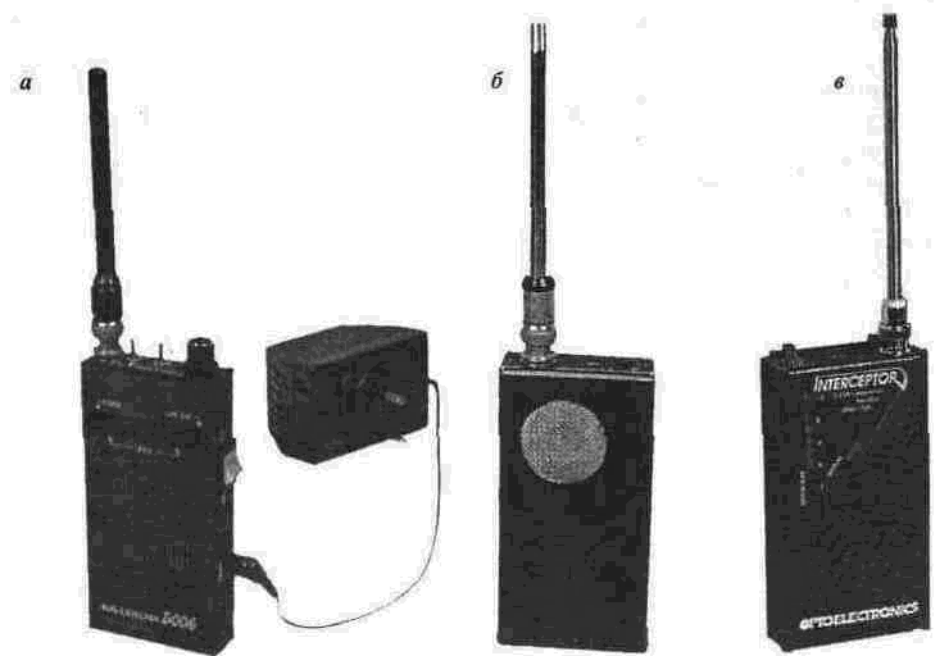



**Рис. 2.3.6. Индикаторы поля:**
а — D006; б — ИП-4М; в — Interceptor RIO

**Таблица 2.3.1. Технические характеристики наиболее распространенных индикаторов поля**

Модель /Диапазон, МГц /Вес, кг /Питание, В /Габариты, мм /Время непрер. работы, ч /Индикация /Аку-стич. завязка
//////световая /звуковая /

DAR-1 DAR-1 /0,05...1300 0,05... 12000 /4,1 4,1 /— /29x23x11 29x23x11 /12 12 /+ + /+ + /+ +
РК870 /1...1000 /0,2 /9 /135x70x20 /45 /+ /+ /—
DM-5 /1...1000 /0,4 /9 /156x38x75 /20 /+ /+ /—
DM-15 /1...1800 /0,15 /9 /62x26x78 /5 /+ /+ /—
VLP5000 /2...1500 /0,4 /2x9 /140x77x34 /8 /+ /+ /+
DM-1 /5...1500 /0,47 /9 /138x75x8 /— /+ /+ /—
MT102 /10...1000 /— /3 /100x62x21 /— /+ /+ /—
DM-6 /10... 1000 /0,31 /9 /56x89x22 /— / /вибро /—
DM-12 /10...4000 /4 / /250x240x110 /— /+ /+ /+
DM-2 /20...1000 /0,8 /9 /150x40x19 /— /+ /+ /+
ШИП /20...1000 /— /— /— /28 /+ /+ /+
UM-063,1 /20...1000 /0,2 /9 /160x70x20 /28 /+ /+ /—
UM-063,2 /20...1000 /0,15 /6 /124x68x27 /100 /+ /+ /—

UM-063,3 /20...1000 /0,19 /9 /124x64x21 /30 /+ /+ /—
MR-4 /20...1000 /0,9 /9 /20x15x4 /— /+ /+ /+
ДР306 /25... 1000 /0,1 /4,5 /35x45x15 /3 /+ /+ /—
ДР302 /25...1000 /0,2 /9 /124x64x21 /30 /+ /+ /—
ДР303 /25...1000 /0,9 /9 /220x90x40 /3 /+ /+ /—
UM-015 /25...1000 /0,9 /9 /220x90x40 /3 /+ /+ /—
D-006 /50...1200 /— /9 /128x63x20 /3 /+ /+ /+
ИП-3 /50...1200 /— /9 /140x20x60 /30 /+ /+ /+
СП /60...180 / /9 /160x80x30 /— /+ /+ /+
pt-0,25 /30... 1500 /— /2x9 /164x83x42 /— /+ /+ /+

### 2.3.3. Специальные радиоприемные устройства

**Панорамные приемники и их основные характеристики**

Радиоприемные устройства, безусловно, являются более сложным и более надежным средством выявления радиозакладок, чем индикаторы поля и частотомеры. Однако для того, чтобы быть пригодными к решению задач поиска, они должны удовлетворять трем основным условиям:

>• иметь возможность настройки на частоту работы устройств, скрытно передающих перехваченную информацию;

>• обладать функциями выделения нужного сигнала по характерным признакам на фоне мешающих сигналов и помех;

**>•** обладать способностью к демодуляции различных видов сигналов.

С решением первой задачи практически каждый многократно сталкивался, настраиваясь на свою любимую радиостанцию, правда, при этом зная ее рабочую частоту. О подслушивающем устройстве, по вполне понятным причинам, известно только то, что оно, скорее всего, работает в диапазоне 20... 1500 МГц. То есть используемый приемник должен, как минимум, перекрывать весь этот частотный интервал. Однако если посмотреть на шкалу своего домашнего тюнера и сравнить его рабочие частоты с требуемыми, то легко увидеть, что даже самые дорогие первоклассные бытовые системы не перекрывают и сотой доли необходимого диапазона.

Следовательно, для надежного обнаружения радиозакладок нужен специальный приемник, позволяющий контролировать чрезвычайно большой набор частот, причем делать это он должен либо одновременно во всем диапазоне, либо перестраиваясь от значения к значению за предельно малый промежуток времени. Такие системы получили название панорамных.

Для решения второй задачи приемник должен иметь полосу пропускания $\Delta f_{п}$ (интервал частот в пределах которого ведется прием), приблизительно равную ширине спектра сигнала $\Delta f_{сп}$ ($\Delta f_{п} \approx \Delta f_{сп}$).

Спектр — это своеобразный частотный портрет электромагнитного излучения, который обычно представляют графически в декартовой системе координат в виде набора вертикальных составляющих. Их положение на оси ординат характеризует абсолютное значение частоты, а высота — амплитуду, значение которой определяется по оси абсцисс.

Задача приемника состоит в том, чтобы «вырезать» из всего многообразия частот интервал, соответствующий спектру принимаемого сигнала и подавлять все, что находится за его пределами. Качество выполнения этой операции характеризуется так называемой избирательностью.

Для ясного понимания проблем, связанных с решением третьей задачи, следует иметь представление о том, что с физической точки зрения звук человеческой речи представляет собой акустические колебания воздуха, частота которых не превышает нескольких килогерц. Передавать их на большие расстояния невозможно, поэтому с помощью микрофонов эти колебания преобразуют в электрические, после чего применяют так называемую модуляцию. При осуществлении процесса модуляции сигнал звуковой частоты как бы совмещают с высокочастотным радиосигналом, и

последний переносит полезную информацию в точку приема. Отсюда и название несущая для высокочастотного излучения. «Слияние» двух типов колебаний осуществляется за счет того, что по закону, диктуемому низкочастотным сигналом, меняется какой-нибудь параметр высокочастотного. Когда изменяется амплитуда, то модуляция называется амплитудной (АМ), когда частота — частотной (FM) и т. д.

Указанное изменение (модуляция) приводит к тому, что передатчик излучает не одну частоту fo своего генератора, а целый набор, который включает в себя не только несущую, но и все частоты звукового сигнала, расположенные справа и слева от несущей в полосе Δfсп. Радисты обычно называют их боковыми составляющими. Общий вид спектра амплитудно-модулированного сигнала представлен на рис. 2.3.7, а.

Именно эти боковые составляющие и содержат полезную информацию. В радиоприемном устройстве избавляются от несущей, а полезный сигнал снова преобразуют в низкочастотный — его демодулируют с помощью детектора, соответствующего типу использованной модуляции. Для демодуляции АМ-сигнала, в принципе, достаточно иметь только одну боковую полосу, поэтому с целью уменьшения ширины спектра Δfсп излучения передатчика иногда применяют однополосную модуляцию (SSB). В этом случае «отрезается» правая или левая боковая составляющая (рис. 2.3.7, б). Справедливости ради надо отметить, что в ряде случаев и несущая, не обладающая никакой полезной информацией, ослабляется или просто подавляется (рис. 2.3.7, в).

При частотной модуляции процесс формирования спектра немного сложнее, а его вид зависит от индекса модуляции mf — соотношения между величиной изменения частоты несущего колебания Δfo и максимальным значением модулирующей частоты Fmax(mf=Δfo/Fmax). Если индекс mf меньше единицы (mf<1), то спектр практически не отличается от спектра АМ-сигнала (рис. 2.3.7, а). При больших индексах модуляции (mf>>1) отличия становятся более существенными, но общая структура (наличие двух боковых полос) остается неизменной (см. рис. 2.3.8, а).

Весьма характерным является и вид спектра радиозакладных устройств, в которых применено цифровое кодирование передаваемой информации. Огибающая спектра такого высокочастотного излучения описывается функциональной зависимостью, известной как sin x/x. Вид его на экране анализатора спектра показан на рис. 2.3.8, б.

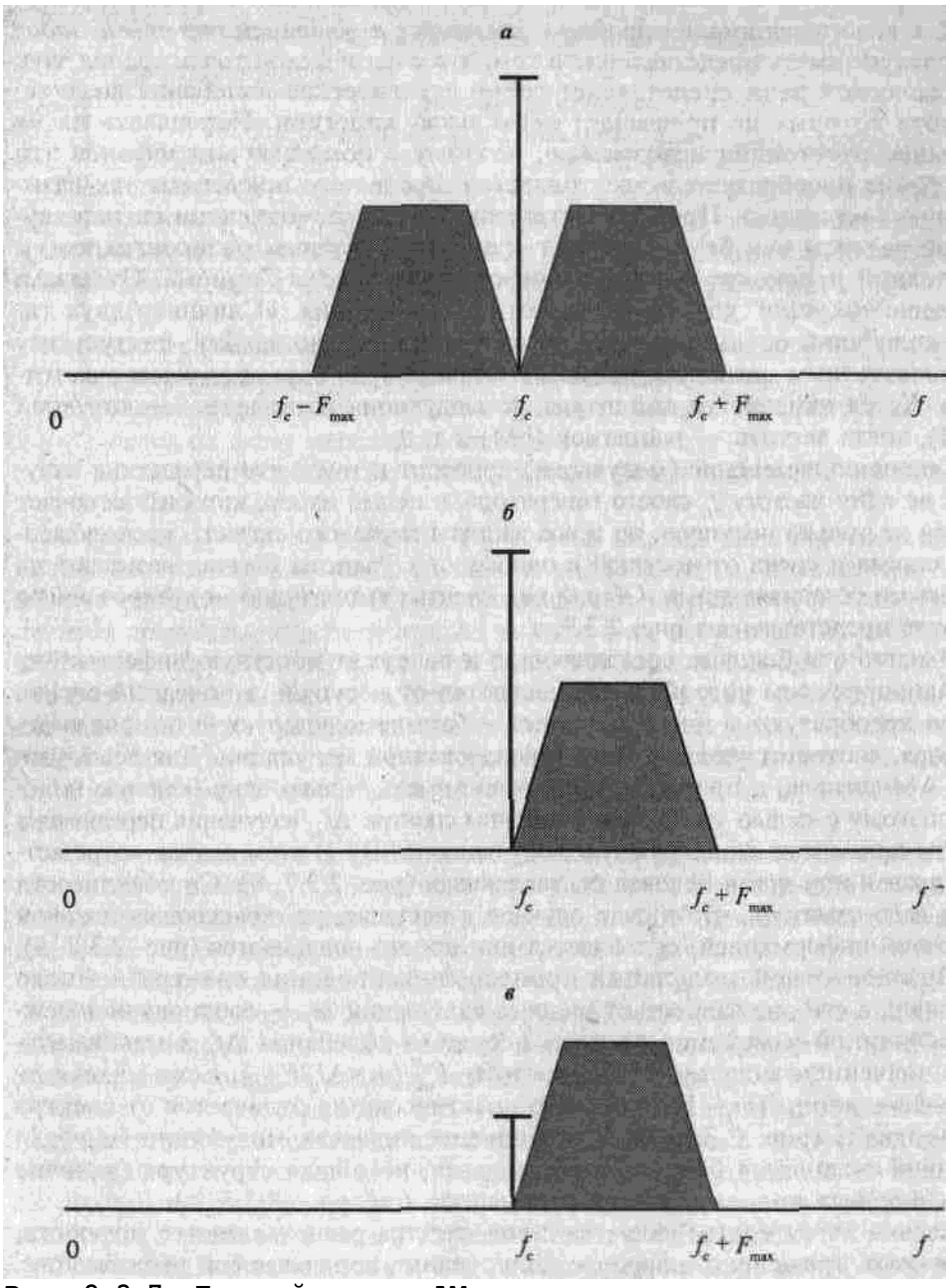



**Рис. 2.3.7. Типовой спектр АМ-сигнала:**
а — общий вид; б — однополосный сигнал; в — однополосный сигнал с ослабленной несущей

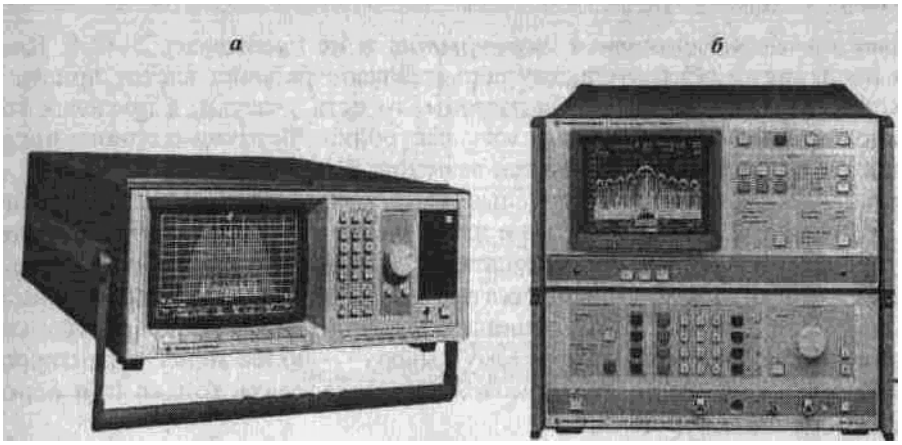



**Рис. 2.3.8. Спектры сигналов со сложными видами модуляции:**
а — частотно-модулированного сигнала при большом индексе модуляции (mf>> 1); б — сигнала с цифровым кодированием передаваемой информации

Как было отмечено выше, полоса пропускания приемника должна соответствовать ширине спектра сигнала, однако она, в свою очередь, зависит от добротности системы и значения несущей частоты. На высоких частотах (100 МГц и выше) требуемую полосу сформировать практически невозможно и, поэтому применяют так называемое преобразование (уменьшение) частоты принятого сигнала с помощью специального генератора (гетеродина). Эта операция выполняется в специальном каскаде-смесителе, а уменьшенная частота называется промежуточной, ее значение, как правило, лежит в диапазоне 200...500 кГц.

Перестройка приемника в пределах заданной области частот осуществляется путем одновременного изменения параметров гетеродина и входных высокочастотных (ВЧ) фильтров. Такое техническое решение обеспечивает постоянную разность между частотами гетеродина и принимаемого сигнала, равную значению промежуточной частоты. Если диапазон перестройки невелик, то сделать такую систему не представляет особой трудности, но в панорамных приемниках — это очень сложная проблема.

Судите сами, изменение частоты настройки производится путем изменения параметров элементов, входящих в состав фильтра или контура гетеродина. Эти детали так и называют — переменные, обычно это конденсаторы или их аналоги. Однако в природе нет таких радиоэлементов, которые могли бы плавно менять свою величину в очень больших пределах: теоретически можно получить отличие максимального значения от минимального в 3 или 3,5 раза, а на практике и того меньше. Поэтому наибольшая частота, на которую настроена избирательная система, тоже отличается от наименьшей не так сильно, как нам бы хотелось. Это отношение называется коэффициентом перекрытия и не превышает 2—2,5. Благодаря последнему обстоятельству весь диапазон рабочих частот приемника приходится разбивать на поддиапазоны, то есть участки, в пределах которых можно плавно изменять частоту настройки. Переход с одного поддиапазона на другой осуществляется заменой ВЧ-фильтра. В принципе, эту операцию вы многократно проделывали, переключая свой бытовой приемник, например, с СВ на УКВ, но в панорамных системах таких поддиапазонов приходиться делать более десятка и, конечно, нужны специальные алгоритмы, по которым должен вестись поиск сигнала. Мы намеренно так детально описали проблемы, возникающие при создании аппаратуры контроля, чтобы подвести вас к простому выводу — более менее гарантированное обнаружение радиозакладок можно осуществить только при использовании специальной техники.

**Принципы построения специальных приемников**

Возможности панорамных приемников в значительной степени определяются методом анализа частотного диапазона. От него полностью зависит и вид структурной схемы. Различают методы параллельного и последовательного анализа.

При параллельном анализе все сигналы, находящиеся в определенной полосе частот, называемой полосой обзора, обнаруживаются одновременно. Структурная схема такого приемника приведена на рис. 2.3.9.

Здесь ВЧ-фильтр 1 формирует требуемую полосу обзора, в которой ведется обнаружение сигналов; смеситель 2 выполняет линейный перенос спектра принятого излучения в низкочастотную область радиодиапазона;

полосовые фильтры 3 — осуществляют частотное разделение сигналов. Выходной усилитель 4 обеспечивает требуемый уровень сигнала, достаточный для нормальной работы анализирующего устройства 5.

Такая структура делает возможным практически мгновенное обнаружение сигналов в полосе обзора при условии, что их уровень превышает пороговую чувствительность приемника. Однако не сложно посчитать, что если контролируемый диапазон частот простирается хотя бы от 20 до 1500 МГц, то при ширине спектра модулированного речью сигнала 5...10 кГц потребуется от 2000 до 300 000 каналов. Ясно, что сделать такую систему, способной «брать» любую радиозакладку, практически нереально из-за ее колоссальной сложности, а значит и стоимости.

В радиоприемнике последовательного анализа, соответственно, осуществляется последовательная перестройка в полосе обзора и обнаружение сигнала. Упрощенная структурная схема устройства подобного типа показана на рис. 2.3.10.

Здесь ВЧ-фильтр 1 имеет полосу пропускания, равную полосе обзора, а гетеродин 3 обеспечивает перестройку приемника в заданной полосе. Про-

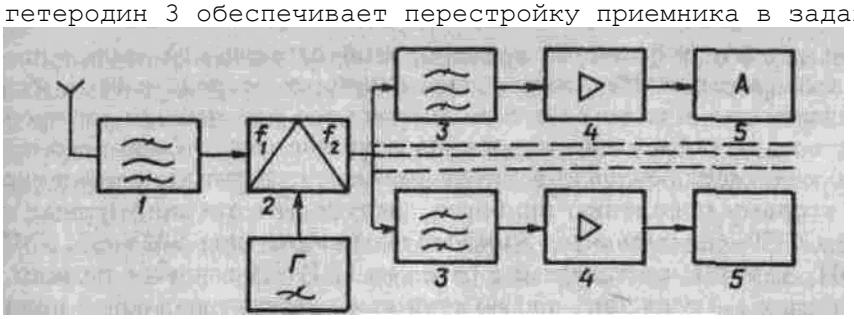



**Рис. 2.3.9. Структурная схема панорамного приемного устройства с параллельным анализом сигналов**

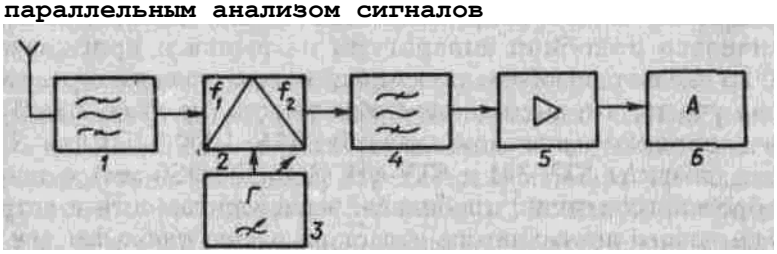



**Рис. 2.3.10. Структурная схема панорамного радиоприемного устройства с последовательным анализом**

межуточная частота — фиксированная. После селекции фильтром 4 и усиления усилителем 5 обнаруженный сигнал поступает в анализирующее устройство 6. При автоматической перестройке приемник как бы «прощупывает» (сканирует) частотный диапазон, отсюда и его обиходное название — сканер. Термин не совсем точный, но весьма распространенный.

**Основные виды панорамных приемников**

Панорамные приемники последовательного анализа в своем развитии прошли несколько этапов.

У нас в стране аппаратура первого поколения представляла собой ламповые

устройства типа **Р-113, Р-250** или **Р-375,** обеспечивающие прием сигнала в определенных частотных диапазонах. В свою очередь, каждый из них имел 8...12 поддиапазонов. Проверка на наличие несанкционированных излучений сводилась к тому, что последовательно прослушивались все проверяемые частотные интервалы. Переключение с поддиапазона на поддиапазон и перестройка гетеродина осуществлялись оператором вручную. В качестве индикатора обнаружения сигнала использовались обычные наушники. Эта аппаратура имела прекрасные технические параметры (например, чувствительность не хуже 0,2...0,3 мкВ, возможность регулировки полосы пропускания и др.), но требовала высочайшей квалификации персонала и очень большого времени, необходимого для проведения полноценной проверки. Некоторые типы подобных устройств из-за их высокой надежности, а часто просто по инерции все еще используют профессионалы, но для любителей данная аппаратура не может быть рекомендована, ибо она имеет неудовлетворительные массогабаритные характеристики.

Ко второму поколению приборов следует отнести популярные в 80-е годы в СССР селективные микровольтметры типа **SMV-6,5, SMV-8,5, STV-301, STV-401,** поставляемые ранее из ГДР. Название не должно никого вводить в заблуждение, ибо по сути они представляют собой полноценные супергетеродинные приемники с собственным генератором развертки, обеспечивающим визуальное представление зависимости уровня принимаемого сигнала от частоты в широком динамическом диапазоне. Значительное количество подобной аппаратуры на рынке и приемлемая цена (100...1000 $) делает подобные приемники весьма привлекательными. Особенно если учесть, что высокая чувствительность (не хуже 2 мкВ) обеспечивается в широком частотном диапазоне (26... 1000 МГц для SMV-8,5). Небольшие габариты **STV-301 и STV-401** (360x320x130 мм), а также наличие калиброванных антенн, пробников, эквивалентов сети и встроенного никель-кадмиевого аккумулятора делает их очень удобными для мобильной эксплуатации. Однако недостаточно широкий диапазон контролируемых частот уже не отвечает современным требованиям. Поэтому для серьезной проверки данную аппаратуру применять не следует, поскольку целый ряд весьма распространенных типов «подслушек» находится за пределами «сферы интересов» этих приемников.

В конце 1992 года на отечественном рынке появилась аппаратура третьего поколения — сканирующие приемники, в основном японского или немецкого (ФРГ) производства. Сначала потенциальных покупателей отталкивала их достаточно высокая цена (до 2500 $), однако несомненные достоинства подобной аппаратуры быстро сделали ее популярной как у опытных специалистов, так и у «юниоров». Сканирующие приемники можно разделить на две группы: носимые и возимые.

К первой группе (носимых) относятся малогабаритные приемники весом 150...300 г, выполненные в корпусе, удобном для скрытого ношения (типа сотового телефона первых моделей) и пригодные для работы в любых условиях. Они имеют автономные источники питания и свободно умещаются во внутреннем кармане пиджака. Однако несмотря на малые размеры и вес подобные приемники позволяют вести контроль в диапазоне частот от 100 кГц до 1300 МГц, а некоторые и до 2000 МГц **(AR-8000, HSC-050).** Они обеспечивают прием сигналов с амплитудной (АМ), узкополосной (NFM) и широкополосной (WFM) частотной модуляцией. Приемник **AR-8000,** кроме того, позволяет принимать сигналы с амплитудной однополосной модуляцией (SSB) как в режиме приема верхней (USB), так и нижней боковой полосы (LSB), а также телеграфных сигналов (CW). При этом чувствительность составляет, в зависимости от вида сигнала, от 0,35 до 6 мкВ. Портативные сканирующие приемники имеют от 100 до 1000 каналов памяти и обеспечивают скорость сканирования от 20 до 30 каналов за секунду при шаге перестройки от 50 Гц до 1000 кГц. Практически все они могут

управляться компьютером. Характеристики некоторых переносных сканирующих приемников приведены в табл. 2.3.2.
Возимые приемники отличаются от переносных несколько большим весом — от 1,2 до 6,8 кг, габаритами и, в некоторых случаях, имеют дополнительные возможности. Они предназначены для работы в помещениях или автомобиле. Почти все приборы этого типа имеют возможность управления с ПЭВМ. Характеристики некоторых, наиболее популярных у специалистов (данные 1998 года), перевозимых сканирующих приемников приведены в табл. 2.3.3.
В несколько обособленный подкласс возимых приемников можно выделить сканеры, выпускаемые либо в виде специальных блоков, которые подключают к ПЭВМ, или в виде печатных плат, вставляемых непосредственно в системный блок компьютера. В качестве примера реализации подобной аппаратуры могут служить устройства **IC-PCR1000 и Winradio.**
Приемник **IC-PCR1000** выполнен в виде отдельного блока и работает под управлением ПЭВМ через встроенный компьютерный интерфейс RS-232C. Сканер имеет шумоподавитель, функции автоматической подстройки частоты и остановки сканирования при обнаружении модулированного сигнала. В комплект входит специальное программное обеспечение для Windows-95. Панель управления выводится на экран монитора (рис. 2.3.11)
Его основные технические характеристики:
**>•** автоматическое сканирование в заданном диапазоне частот; рабочий диапазон частот—0,01...1300 МГц;
>• автоматическое сканирование в заданном диапазоне частот; виды модуляции принимаемых сигналов — USB, LSB, CW, AM, FM и WFM;
>• автоматическое сканирование в заданном диапазоне частот; количество каналов памяти — практически неограниченное;
**>•** автоматическое сканирование в заданном диапазоне частот; минимальное разрешение по частоте — 1 Гц;
**>•** автоматическое сканирование в заданном диапазоне частот; режим перестройки параметров приема при выборе частот — автоматический;
**>•** автоматическое сканирование в заданном диапазоне частот; размеры блока — 127x30x199 мм;
>• автоматическое сканирование в заданном диапазоне частот; вес — 1 кг.
Универсальный сканирующий приемник **Winradio** выполнен в виде печатной платы ISA IBM размером 294x121x20 мм. Он имеет режим автоматического сканирования в пределах диапазона 500 кГц... 1300 МГц. Скорость


**Рис. 2.3.11. Вид программной оболочки приемника IC-PCR1000**

сканирования 50 каналов/с. Чувствительность — 0,5 мкВ. Позволяет отображать на экране дисплея ПЭВМ спектрограммы и осциллограммы принимаемых сигналов и давать сведения об их уровне. Шаг перестройки по

частоте может быть установлен в пределах от 1 кГц до 1 МГц. Панель управления также отражена на экране монитора.
Аппаратура данного типа представляет собой нечто промежуточное между обычными приемниками и специализированными автоматизированными комплексами по поиску радиозакладок, о которых будет подробно рассказано в следующем подразделе.
Обычные сканирующие приемники (как носимые, так и возимые) могут работать в одном из следующих режимов:
>• автоматическое сканирование в заданном диапазоне частот;
>• автоматическое сканирование по фиксированным частотам;
>• ручной режим.
Первый режим работы является основным при поиске излучений радиозакладок. В этом случае устанавливаются начальная и конечная частоты сканирования, шаг перестройки и вид модуляции. Существенным преимуществом данного режима является то, что сканирование можно осуществлять с пропуском частот постоянно работающих в этом районе радиостанций (например, всех программ телевидения, городской трансляционной сети и т. д.). Они хранятся в специально выделенных для этих

**Таблица 2.3.2. Носимые сканирующие приемники**

Наименование характеристик /Индекс (тип)
/«C-R1 /IC-R10 /DG-X1 D /AR-2700 /AR-8000
фирма-изготовитель /1C /OM /ALINCO /AOR /AOR
Диапазон частот, МГц /0,1...1300 /0,5...1300 /0.1...1300 /0,5... 1300 /0,5...1900
Виды модуляции /AM, NFM, WFM /AM, NFM, WFM, SSB /AM, NFM, WFM /AM, NFM, WFM /AM, NFM, CW, WFM, LSB.USB
Чувствительность при отношении сигнал/шум 10 дБ, мкВ /AM: 0,8...1,6 NEM: 0,4...0,8 WFM: 3,2...6,3 /AM: 1,0...2,0 NFM: 0,35...0,79 WFM: 1,0...2,0 SSB: 0,25...0,63 /AM:.0,8...1,6 NFM: 0,4...0,8 WFM: 3...6,3 /AM: 1,0...3,0 NFM: 0.5...1.5 WFM: 1,0...6,0 /AM: 1,0...3,0 NFM; 0,35...3,0 WFM: 1,0...1,6 SSB: 0,26... 1,0
Избирательность на уровне 6 дБ, кГц /AM, NFM:15 WFM:150 /AM, NFM: 15 WFM: 150 SSB: 2,4 /AM, NFM: 15 WFM: 50 /AM, NFM:12 WFM: 180 /AM, NFM: 12 WFM: 180 LSB, USB: 2,4
Шаг перестройки частоты, кГц /0,5; 5; 8; 9; 12,5; 15; 20; 25; 30; 50; 100 /5; 8; 9; 12,5; 15; 20; 25; 30; 50; 100 /5; 6,25; 9; 12,5; 15; 20; 25; 30; 50; 100 /Кратный 50 Гц
Число каналов памяти /100 /100 (в 18 банках) /100 /По 50 (в 10 банках) /По 50 (в 20 банках)
Скорость сканирования, канал/с /10(20) /20 /10; 15; 20 /20...30
Выходы приемника /Головине телефоны /Головные телефоны, IBM PC /Головные телефоны /Головные телефоны; IBM PC
Питание, В /DC 7,8 (аккумулятор) DC 6...15 (внешнее) /DC б (4XAA) DC 4,5-16 (внешнее) /DC 7,8 (аккумулятор) DC 6...15 (внешнее) /DC4.8 (Ni-Cd батарея) DC 6(AA) DC 6...16 (внешнее)
Размеры, им /49 xl03 x35 /59x130x32 /53x110x37 /69x153x40
Масса, г /280 /310 /370 (без антенны) /350 (без антенны)

**Таблица 2.3.3. Возимые сканирующие приемники**

Наименование характеристик /Индекс (тип)
/IC-R100 /AR-MOOA /1C-R8500 /AR-5000
Фирма-изготовитель /ICOM /AOR /ICOM /AOR
Диапазон частот, МГц /0,1-1300 /0.1...2036 /0,1...2000 /0,01...2600
Виды модуляции /AM,NFM, WFM /AM, NFM, WFM, LSB, USB, CW /AM, FM, NFM,

WFM, LSB, USB, CW, AM-N /AM, FM, LSM, USB, CW

Чувствительность при отношении сигнал/шум 10 дБ, мкВ /AM: 0,6-3,2 NFM: 0,2-0,56; WFM: 0,6-1,5 /AM: 0,1-3,2; NFM: 0,35-1,5; WFM: 1,0-6,0; LSB: 0,25-1,0 /AM; 2,5-6,3; NFM: 0,5; WFM: 1,4-2,0; USB; 0,25-1,0 /AM: 0,36-0,56; FM: 0,2-1,25; SSB: 0,14-0,25

Избирательность на уровне 6 дБ, кГц /AM: 6; NFM: 15; WFM: 150 /AM, NFM: 12; WFM: 180; LSB, USB: 2,4 /AM: 5,5; FM: 12; WFM: 150 /3; 6; 15; 40; 110; 220

Шаг перестройки, кГц /1; 5; 8; 9; 10; 12,5; 20; 25; 100; 1000 /Кратный 50 Гд /0,01; 0,05; 0,1; 1; 2,5; 5; 10; 12,5; 20; 25; 100; 1000 /Or 1 Гц до 1 МГц

Число каналов памяти /21 /По 100 (в 4 банках) /1000 /1000

Питание, В /Внешнее /Внешнее /Внешнее /Внешнее

Размеры, мм /150x50x181 /130x80 x200 /287x112x309 /204 x77 X240

Масса, кг /1,4 /1,2 /7,0 /3.5

Скорость сканирования, канал/с /20 /30(50) /40 /50

Выходное устройство /Головные телефоны /Головные телефоны; ПЭВМ /Головные телефоны; магнитофон; ПЭВМ /Головные телефоны; ПЭВМ

целей ячейках памяти. Наличие данной функции существенно сокращает время просмотра выбранного диапазона частот при поиске радиозакладок.

В зависимости от квалификации оператора можно использовать несколько режимов автоматического сканирования:

>• автоматическое сканирование в заданном диапазоне частот; при обнаружении любого сигнала (превышении им уровня установленного порога) сканирование прекращается и возобновляется только после подачи оператором соответствующей команды;

>• автоматическое сканирование в заданном диапазоне частот; при обнаружении сигнала сканирование останавливается и возобновляется после его пропадания;

>• автоматическое сканирование в заданном диапазоне частот; при обнаружении сигнала сканирование останавливается для принятия решения и автоматически возобновляется по истечении нескольких секунд. В ряде моделей этот интервал регулируемый, например, для приемника AR-3000A время паузы может изменяться от 1 до 9 с.

Второй режим используется для ведения радиоразведки, когда известны и записаны в каналы памяти возможные частоты работы радиосредств. Думаем, не надо быть специалистом, чтобы догадаться, что именно этот режим применяют в случае, когда панорамный приемник используется для приема сигнала от своей радиозакладки. Поэтому включение аппаратуры этого типа в разделы 1.3 и 1.5 (например, табл. 1.5.3) совсем неслучайно.

Третий режим работы применяется для детального обследования всего или отдельных участков частотного диапазона и отличается от первого тем, что перестройка приемника осуществляется оператором с помощью ручки изменения частоты, при этом информация о частоте настройки, виде модуляции, уровне входного сигнала и т. д. выводится на встроенный дисплей. Основным недостатком данного режима является очень малая скорость просмотра диапазона и, как следствие, возможность пропуска сигнала.

Перестройка по частоте в любом из перечисленных режимов идет с постоянным, заранее выбранным шагом. Ясно, что при поиске закладки этот шаг должен быть соизмерим с шириной спектра искомого сигнала. Кроме того, поиск должен осуществляться отдельно для каждого вида возможной модуляции сигнала.

У ряда приемников на дисплее кроме информации о частоте настройки и виде модуляции отображается уровень принимаемого сигнала. В частности,

у приемника **AR-3000A** уровень входного сигнала отображается в виде 9-сегментной диаграммы (как на эквалайзере музыкального центра). При этом первый сегмент примерно соответствует уровню 10 мкВ, седьмой — 30 мкВ, а девятый — 300 мкВ. Более детально проанализировать сигнал можно с помощью специальной панорамной приставки, например **SDU-5000.**

Для придания большей практической направленности сведениям, полученным из этого краткого обзора, рассмотрим более подробно некоторые, на наш взгляд, наиболее распространенные модели панорамных приемников.

**Модели панорамных приемников**

Возимый приемник AR-3000A

Заслуженной популярностью на рынке спецтехники пользуется приемник AR-3000A японской фирмы A.O.R Ltd, который отлично зарекомендовал себя в условиях России. Стоимость его довольно высока — 1200...1500 $, но на вторичном рынке она существенно ниже, поскольку прибор завезен к нам в большом количестве. Внешний вид прибора можно видеть на рис. 2.3.12.

Это удобный приемник, имеющий достаточно широкие возможности. Он может работать как от сети 220 В, так и от бортовой сети автомобиля, для чего в комплект входит разъем подключения к гнезду «прикуривателя» — AR-3000A специально создавался в расчете на установку в салоне машины. Имея такой мобильный пункт радиоконтроля, можно решать задачи самого широкого круга в том числе и за пределами своего офиса. Диапазон приемника охватывает широкий спектр радиоволн — от 100 кГц до 2036 МГц. На момент создания это был самый широкодиапазонный малогабаритный сканер в мире, его структурная схема представлена на рис. 2.3.13.

Весь диапазон разбит на 13 поддиапазонов с помощью набора активных фильтров. Первый фильтр «вырезает» полосу частот от 100 до 500 кГц, а последний, тринадцатый, — от 940 до 2036 МГц. Эти фильтры — подлинная изюминка всех видов радиоаппаратуры указанной фирмы. Благодаря их отменным характеристикам они не только обеспечивают надежное подавление зеркального канала, но и используются в роли усилителя высокой частоты, что позволяет достичь очень высокой чувствительности (0,1 мкВ в режиме АМ). На рис. 2.3.14 приведена амплитудно-частотная характеристика фильтра № 5 (полоса пропускания 30...50 МГц).

Фильтры объединены в 3 блока, с каждого из которых сигнал поступает на свой смеситель, а затем через переключатель на линейку преобразователей частоты. Встроенный синтезатор обеспечивает необходимый набор частот гетеродина и их перестройку в заданных пределах. Управление всеми операциями осуществляет микропроцессор типа UNIT.

Сигнал промежуточной частоты усиливается в усилителе, выполненном на транзисторах 2SC2759, и направляется в блок детекторов. Детекторы различных видов сигналов (АМ, FM, USB и т. д.) включены параллельно, но к выходному устройству подключаются поочередно в зависимости от желания оператора. К приемнику можно присоединить головные телефоны и записывающее устройство.

Достоинством приемника является наличие жидкокристаллического дисплея с подсветкой, часов, внутренних аккумуляторов для питания памяти, стандартного разъема для подсоединения к компьютеру. На рис. 2.3.12 приемник изображен с простейшей штыревой телескопической антенной, однако имеется возможность работать с антеннами различного типа и назна-

**Рис. 2.3.12. Панорамный приемник AR-3000A**

чения. Для поиска радиозакладок наиболее эффективна всеволновая и всенаправленная антенна типа АН-7000. Ее внешний вид приведен на рис. 2.3.15.

Возможность подключения приемника к персональному компьютеру типа IBM PC раскрывает перед пользователем самые широкие перспективы применения AR-3000A в составе различных программно-аппаратных комплексов, в чем можно убедиться, прочитав подраздел 2.3.4.

Приемник достаточно прост в обращении, а если купить его в солидной организации, то в качестве приложения обязательно будет подробная инструкция по эксплуатации на русском языке, которая позволит быстро освоить основные приемы работы. В общем, приобретение этого прибора — неплохое начало в техническом оснащении любой службы безопасности.

Носимый сканирующий приемник IC-R10

Вот уже более 6 лет на рынке спецтехники известна модель **IC-R1**, которую специалисты высоко ценят за качество и малые габариты. Сегодня фирма ICOM начала выпуск новой модели — **IC-R10**, призванной существенно расширить основные функции прототипа. Внешний вид приемника представлен на рис. 2.3.16, а.

Рабочий диапазон частот у этой «крохи» несколько меньше, чем у **AR-3000A** — от 0,5 до 1300 МГц, но вполне достаточен для обнаружения всех видов радиозакладок. Он разбит на 8 поддиапазонов. На верхней границе диапазона предусмотрено трехкратное преобразование частоты (промежуточные частоты составляют: 1-я — 266 МГц, 2-я — 10,7 МГц, 3-я — 0,455 МГц). Блок детекторов обеспечивает прием сигналов практически со всеми видами модуляции. Высококачественный усилитель позволяет получать очень хорошую для такого класса портативных приемников чувствительность — 1...2 мкВ при модуляции АМ. Для удобства в работе расширен набор вариантов ведения сканирования, каждый из двух основных видов (программируемое и по ячейкам памяти) разбит на типы: сплошное, диапазонное, с автоматической записью обнаруженных частот, по ячейкам памяти и видам модуляции.

Впервые в портативных сканерах реализована система VSC (Voice Scan Control) — интеллектуальное устройство поиска голоса, наличие которой позволяет игнорировать все немодулированные и шумоподобные сигналы. Этот режим чрезвычайно удобен при ведении оперативного радиоконтроля,

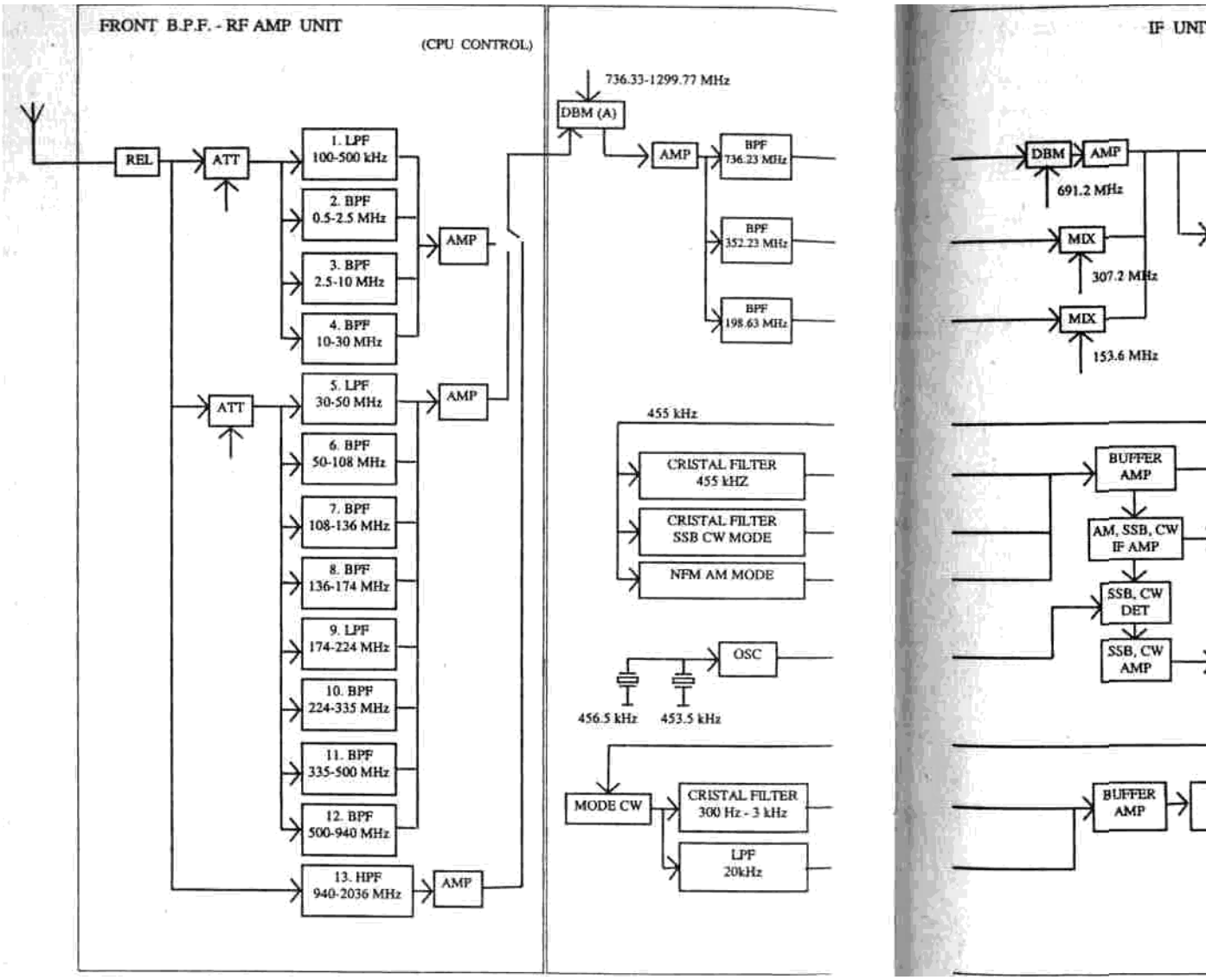



**Рис. 2.3.13. Структурная схема приемника AR-3000A**

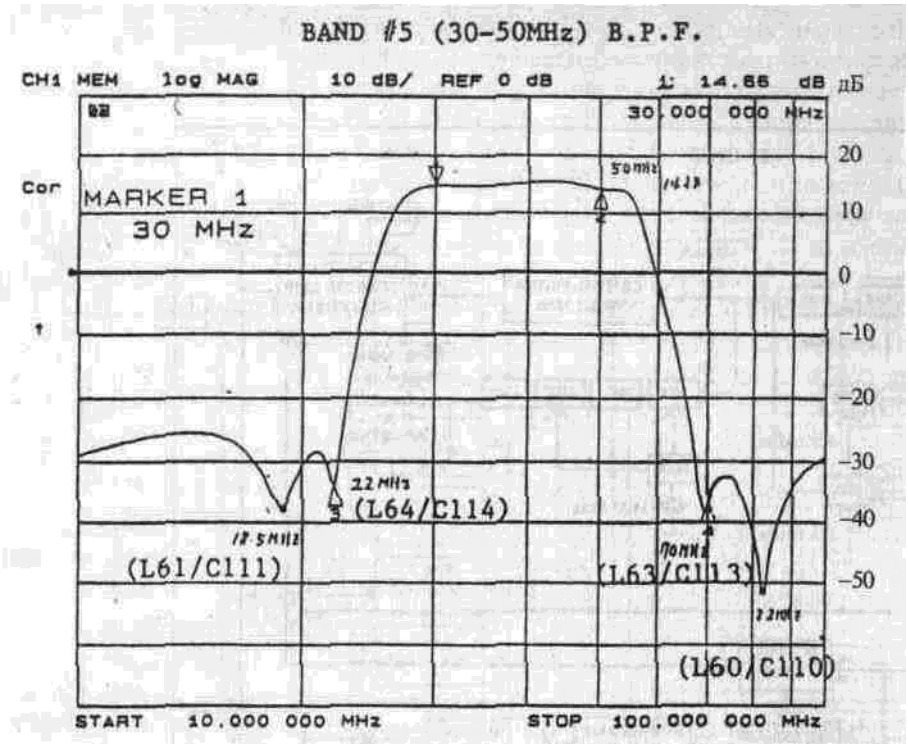



**Рис. 2.3.14. Амплитудно-частотная характеристика высокочастотного фильтра приемника AR-3000A**

например, по ходу совещания или переговоров. Если за несколько минут до начала мероприятия пройти весь диапазон и исключить из поиска частоты постоянно работающих станций, то сканер подаст сигнал тревоги (притом довольно быстро) только при появлении нового сигнала того же вида, что излучает радиозакладка, но не среагирует на излучение от включившегося факса или вдруг заискрившей электророзетки. Большим преимуществом для осуществления такого рода деятельности являются малые размеры и вес.

Значительно сократит время, необходимое для просмотра всего частотного диапазона, наличие еще одной новой функции — SIGNAVI («навигатор сигналов»), которая позволяет в несколько раз увеличить реальную скорость сканирования. В этом случае используется дополнительный приемный контур, который продолжает просмотр диапазона в то время, пока вы остановились на сигнале, обнаруженном основным приемником, и пытаетесь выяснить его происхождение. Таким образом, приемник будет сканировать как бы скачками только по занятым каналам. Правда, величина скачка не сможет превысить 100 кГц.

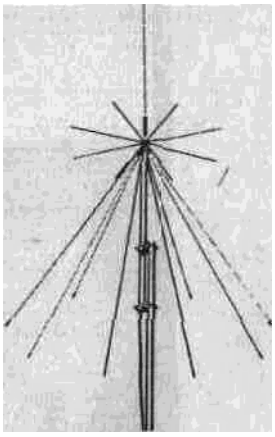


**Рис. 2.3.15. Антенна АН-7000**

Впервые на портативном приемнике имеется спектроскоп, работающий в реальном масштабе времени, что позволяет постоянно контролировать наличие сигналов в полосе частот шириной до 200 кГц (с шагом 20 кГц).

Приемник может быть подключен к компьютеру и управляться им. Обмен данными происходит в формате CI-V через дополнительный блок-интерфейс CT-17. Для подсоединения последнего предусмотрено специальное гнездо.

Питание осуществляется от четырех элементов типа АА или никель-кадмиевого аккумулятора. Размеры (без антенны) — 58,5x130x31 мм, вес — 310 г. Цена — до 600 $.

Внешний вид ряда радиоприемных устройств фирмы ICOM приведен на рис. 2.3.16.

Выше описанные приемники относятся к так называемым приемникам среднего класса — весьма эффективным, но относительно недорогим и не слишком «навороченным». Для богатых клиентов больший интерес может вызвать аппаратура немецкой фирмы «Роде и Шварц», которая стоит очень дорого, но позволяет не только фиксировать факт наличия в помещении подслушивающего устройства, но и приблизительно определять его местоположение. Ясно, что информация такого рода — неоценимое подспорье для поиска закладок с помощью, например, индикатора поля или нелинейного локатора. По своим возможностям лучшие приемники этой фирмы сопоставимы с автоматизированными комплексами (п. 2.3.4).

В качестве примера приведем данные приемников типа **ESP**, которые перекрывают очень широкий частотный диапазон (ESP-T1 — от 10 кГц до 1300 МГц, а ESP-T2 — до 2300 МГц). Они имеют память на 1000 каналов, чувствительность — до 3 мкВ, шаг перестройки — 1, 7, 5, 25, 100 кГц или 2 МГц. Приемники способны разделить сигналы, отстоящие друг от друга всего на 100 Гц, и работать с любыми видами модуляции. Производится автоматическое распознавание принимаемого сигнала, а при наличии калиброванной антенны — и определение расстояния до его источника. В этом случае в помещении устанавливаются дополнительные эталонные генераторы — скауты, которые входят в комплект. Внешний вид прибора представлен на рис. 2.3.17.

Впрочем фирма «Роде и Шварц» выпускает и относительно простую миниатюрную аппаратуру контроля, например приемник **EB100**. Устройство работает в диапазоне 20... 1000 МГц, который, в свою очередь, разбит активными фильтрами на 5 поддиапазонов (первый от 20 до 108, последний — от 500 до 1000 МГц). Имеются все основные режимы сканирования


**Рис. 2.3.16. Панорамные приемные устройства фирмы ICOM:**
а — IC-R10; б — IC-R100; в — IC-R7000; г — IC-R9000

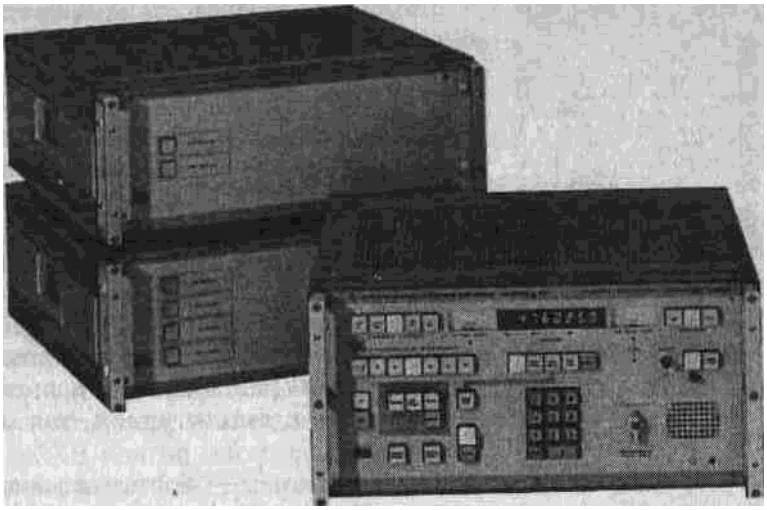


**Рис. 2.3.17. Автоматический приемник ESP**

с шагом от 1 кГц до 10 МГц, принимаются сигналы с модуляцией АМ, FM. Полоса пропускания — 7,5...150 кГц. Питание — комбинированное, от батареи 6 В или от сети 220 В. Внешний вид приемника приведен на рис. 2.3.18.

Если вместе с приемником **EB100** использовать активную остронаправленную антенну НЕ 100, специально созданную для поиска в помещениях радиозакладок, то можно с неплохой точностью определять и местоположение источника излучения. Антенна представляет собой три сменных модуля (рис. 2.3.19) и работает в диапазоне 20... 1000 МГц. Первый модуль перекрывает диапазон от 20 до 200 МГц, третий — от 500 до 1000 МГц.

Среди радиоприемных устройств следует выделить анализаторы спектра, которые позволяют получать частотный портрет сигнала за счет того, что принятый сигнал как бы последовательно просматривается специальным узкополосным фильтром, выводя данные на экран устройства. Развертка синхронизирована с перестройкой фильтра, поэтому на изображении с определенным шагом видны составляющие спектра сигнала, амплитуды которых определяются величиной сигнала на той или иной частоте. Ясность и полнота картинки зависят от шага перестройки фильтра и полосы обзора. На рис. 2.3.20 приведен спектр амплитудно-модулированного сигнала, полученный с помощью анализатора спектра **АХ700Е** при трех различных полосах обзора.

Анализаторы спектра незаменимы в качестве аппаратуры контроля, особенно если априорно не известны такие параметры сигнала, как частота, вид модуляции, способ кодирования и т. д. Например, прибор **EZM** («Роде и Шварц») позволяет анализировать сигналы в диапазоне 9 кГц... 13 00 МГц и устанавливать полосу обзора от 1 кГц до 2 МГц. Он совместим с **ЭВМ** и оснащен собственным 9-дюймовым монитором. У изделия АХ700Е данные несколько скромнее: диапазон частот 50... 905 МГц, и цена почти на порядок меньше.

На базе анализаторов спектра фирма «Роде и Шварц» создала целые комплексы контроля, например FSAC (рис. 2.3.21).

Эта аппаратура обладает высокой чувствительностью, позволяет контролировать диапазон частот 100 Гц... 2000 МГц и анализировать сигналы как с амплитудной, так и фазовой модуляцией.

Другой пример — портативный анализатор спектра **HewlIett-Packard** модель **8591E.** Он позволяет производить измерения в полосе от 9 кГц до 1,8 ГГц. Уникальной особенностью приемника является возможность производить анализ состава спектра с помощью быстрого преобразования Фурье в

диапазоне низких частот (30...300 кГц) нажатием всего лишь одной кнопки. В приборе предусмотрены средства программирования и сохранения программ и данных во внутренней памяти объемом до 512 кб. Экранный интерфейс встроенного дисплея подобен Windows программам. В 8591E предусмотрена возможность сопряжения по управлению и выводу данных с персо-

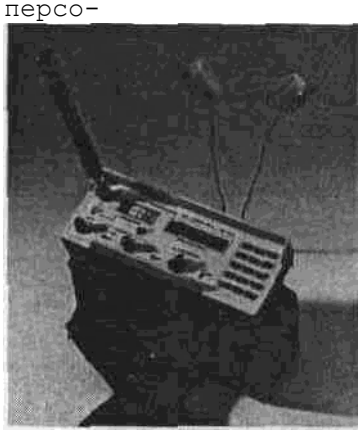


**Рис. 2.3.18. Приемник EB100 фирмы «Роде и Шварц»**

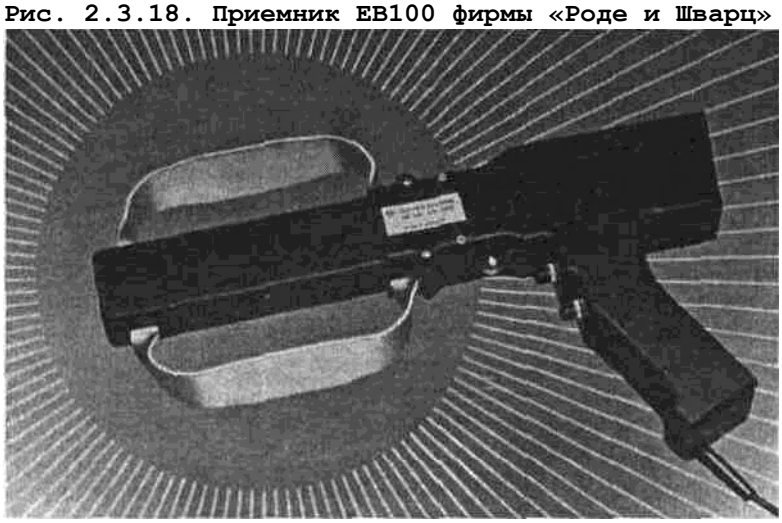


**Рис. 2.3.19. Модуль антенны HE 100**

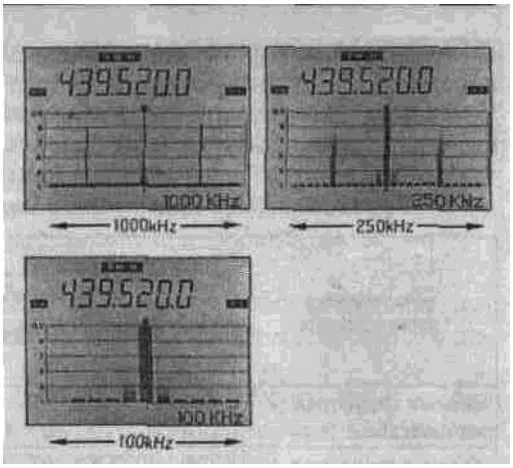



**Рис. 2.3.20. Работа анализатора спектра при различных режимах обзора**

нальным компьютером через шину в стандарте HP-IB или по последовательному интерфейсу формата RS-232. Фирма Hewllett-Packard предлагает новый дешевый портативный спектроанализатор ESA-L1500A,

работающий в диапазоне частот от 9 кГц до 1,5 ГГц с малой погрешностью измерения частоты (±2 кГц на частоте 1 ГГц). Прибор прост в эксплуатации, имеет экранный интерфейс типа Windows и совместим по управлению с персональным компьютером по шине стандарта HP-IB или по последовательному интерфейсу RS-232. В прибор встроен трекинг-генератор для задания среднего значения частоты анализируемого частотного интервала. В зависимости от опций масса прибора варьирует от 12,3 кг до 25 кг.

Панорамный приемник ближнего поля **Belan** разработан отечественными специалистами. Прибор имеет рабочий диапазон от 100 кГц до 2,1 ГГц. По существу он сочетает в себе функции анализатора спектра и поискового комплекса. В нем предусмотрено три режима функционирования. В режиме приемника производится демодуляция амплитудно-модулированных (АМ) или частотно-модулированных (ЧМ) сигналов на выбранной частоте. В режиме спектрального анализа на дисплее индицируется и периодически обновляется изображение модуля спектра сигналов, обнаруженных в полосе сканирования. Режим поиска предназначен для регистрации радиосигналов, амплитуда которых превышает пороговое значение, которое задается оператором. Прибор Belan имеет внутреннюю энергозависимую память, в которой может сохраняться до 1000 значений частот обнаруженных ранее сигналов. Прибор полностью программируется и сопрягается с персональным компьютером по последовательному порту формата RS-232. Он прост в обращении, име-

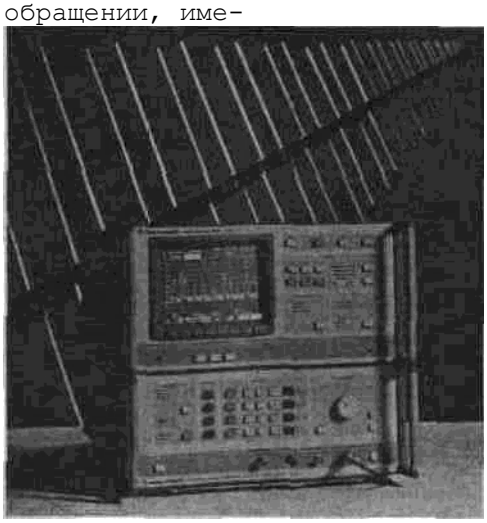


**Рис. 2.3.21. Комплекс контроля FSAC**

ет приятный экранный интерфейс, малую массу (6 кг) и возможность независимого энергопитания.

Сравнительные характеристики некоторых современных анализаторов спектра приведены в таблице 2.3.4.

Таблица 2.3.4. Сравнительные характеристики анализаторов спектра

| Технические характеристики | Фирма–производитель оборудования, модель | | | | | | |
|---|---|---|---|---|---|---|---|
| | Tektronix | | Hewllett-Packard | | Элвира | Rohde&Schwarz | Advantest |
| | 2795 | 2712 | 8561E | ESA-L1500A | Belan | FSA | U3641 |
| Нижняя граничная частота, кГц | 0,1 | 9 | 9 | 9 | 100 | 100 | $ |
| Верхняя граничная частота, кГц | 1.8 | 1,8 | 1,8 | 1,5 | 2,1 | 1,8 | 3 |
| Погрешность изменения частоты | ±6 | ±510 | 3 | 3 | 3 | 0,8 | 5 |
| Разрешающая способность по частоте | 0,16 | 0,28 | 0,55 | 0,2 | 0,05 | 0,16 | 0,1 |
| Паразитная частотная модуляция, Гц | 3 | 100 | 80 | 32 | 20 | 1000 | 60 |
| Динамический диапазон, ДБ | 90 | 80 | 77 | 85 | 80 | 100 | 100 |
| Чувствительность, дБ | 131 | 127 | — | — | 85 | — | 130 |
| Погрешность измерения амплитуды, дБ | 2 | 2 | 1,7 | 1,5 | 2,7 | 1,5 | 2 |
| Относительные уходы частоты опорного генератора | 1E-9 | 1E-9 | 2E-6 | 2E-6 | 2E-8 1E-7 | 5E-10 1E-7 | 2E-8 1E-7 |
| Нелинейнейные искажения, дБс | -60 | -66 | -70 | -75 | -70 | -75 | -70 |
| Интермодуляционные искажения, дБс | -10 | -70 | 70 | 74 | 70 | 75 | 70 |
| Входное сопротивление, Ом | 75/50 | 75/50 | 75/50 | 75/50 | 50 | 50 | 50 |
| Наличие АМ и ФМ демодуляторов | нет | да | да | да | да | да | Да |
| Интерфейсы связи с ПЭВМ | GPIB | GPIB, RS-232 | HP-IP, RS-232, PI | HP-IP, RS-232, PI | RS-232 | RS-232 | RS-232 |
| Масса, кг | 19 | 9,5 | 14,5 | 12,3 | 6 | 50 | 6,1 |
| Независимый источник питания | нет | Аккум. | Аккум. | Аккум. | Аккум. | нет | Аккум. |

**к**

**омпьютерные программы для управления панорамными приемниками**

Функциональное совмещение специальных приемников с персональными компьютерами существенно повышает надежность и оперативность поиска ЗУ, делает процедуру выявления более удобной (технологичной).
На компьютер при этом возлагается решение следующих задач:
>• хранение априорной информации о радиоэлектронных средствах, работающих в контролируемой области пространства и выбранных диапазонах частот;
>• получение программными методами временных и частотных характеристик принимаемых сигналов (вместо использования достаточно громоздких осциллографов и анализаторов спектра);
>• тестирование принимаемых сигналов по совокупности признаков на принадлежность к излучению ЗУ.
На российском рынке в настоящее время известно большое количество программ, специально разработанных для ведения поискового радиомониторинга. Наиболее известные среди них — это **«СканАР»**, **Sedif**, **Filin**, **RSPlus**, **«Крот-mini»**, **Arcon**, **Radio-Search**, а также некоторые другие.
**Программа «СканАР».** Характерным представителем семейства программных продуктов, реализующих вышеуказанные свойства, является программа «СканАР», ее базовая версия имеет четыре основных режима работы:
>• «Панорама» —для анализа загруженности контролируемого диапазона частот, сохранения полученной информации в архиве, сравнения результатов контроля, управления принтером для документирования полученных результатов;
>• «Поиск» — для наблюдения за изменением уровней сигналов в нескольких частотных диапазонах;
>• «Обзор» — для анализа наличия сигналов, превышающих заданный порог в широком диапазоне частот, а также просмотра наличия сигналов и их спектров на выбранных частотах;
>• «Сканирование» — для слежения за состоянием каналов выбранного банка памяти (аналогичен режиму сканирования банков памяти в приемнике).
При переходе из режима в режим программа сохраняет все накопленные данные и предоставляет возможность продолжить работу с места остановки или сначала.
При остановке работы любого режима программа осуществляет прием сигнала на фиксированной частоте с выбранными параметрами. При этом возможна ручная перестройка приемника, изменение вида модуляции принимаемого сигнала, включение/выключение звука, изменение значения аттенюатора и т. д.
Рассмотрим подробно каждый из перечисленных режимов.
**>•** Режим «Панорама». Программа выполняет перестройку приемника в пределах заданной полосы обзора относительно выбранной центральной частоты и представляет результат в виде зависимости уровень/частота (рис. 2.3.22). Горизонтальная полоса на изображений показывает выбранный порог.
В рассматриваемом режиме программой предусмотрены три подрежима работы: «Сигнал»; «Спектр»; «Сравнение панорам».
Подрежим «Сигнал» предназначен для наблюдения за изменением уровня сигнала на фиксированной частоте (рис. 2.3.23).
Подрежим «Спектр» предназначен для подробного анализа спектральных характеристик выбранного сигнала. При этом предусмот-

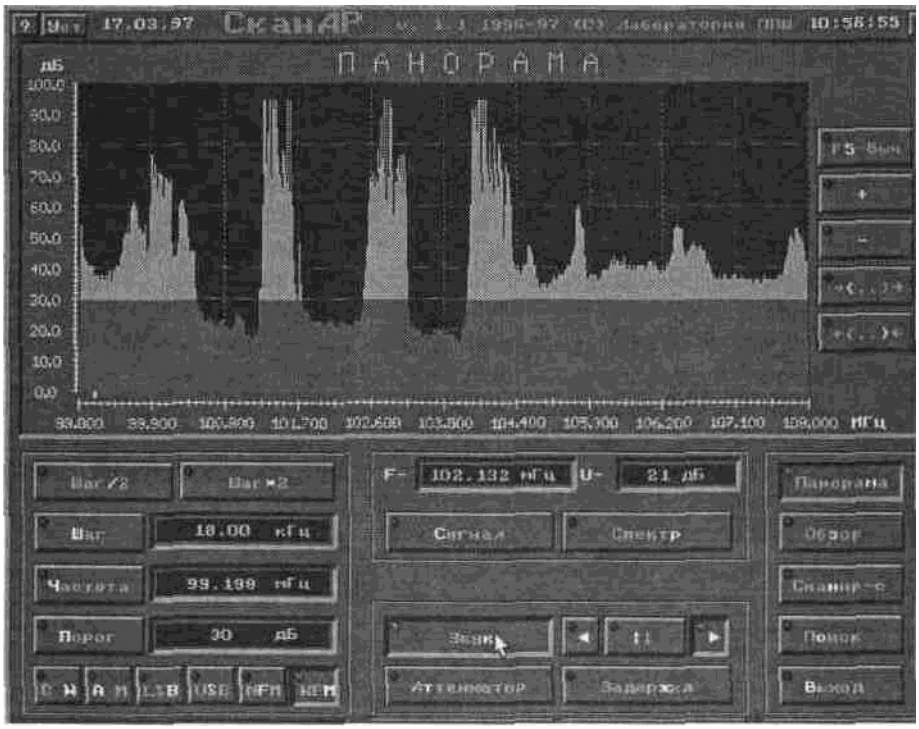



**Рис. 2.3.22. Общий вид экрана в режиме «Панорама»**

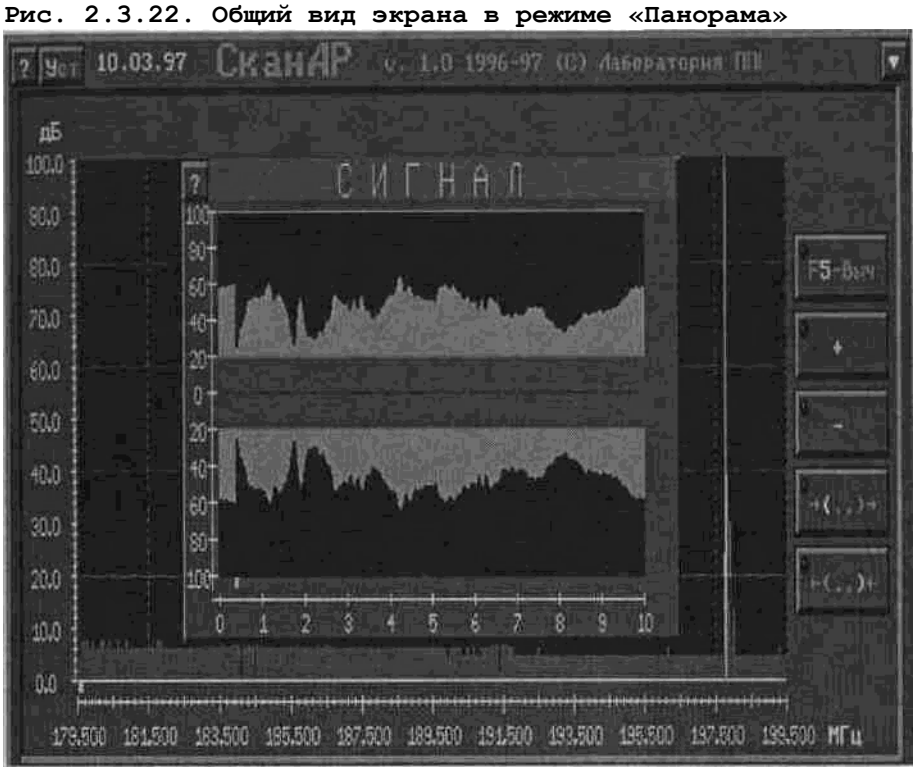



**Рис. 2.3.23. Фрагмент экрана при включенном подрежиме «Сигнал»**

рена возможность изменения ширины области просматриваемых частот и ее положения на оси частот (рис. 2.3.24).

Подрежим «Сравнение панорам» предназначен для сравнения двух панорам — эталонной и текущей. Эталонная хранится в памяти компьютера с запоминанием всех имеющихся установок (центральной частоты, полосы обзора, шага перестройки, полосы пропускания, вида детектора, значения

аттенюатора, порогового уровня), текущая формируется при сканировании того же частотного диапазона.
Например, если в архиве была сохранена определенная панорама, то при загрузке ее из памяти и нажатии клавиши «F5» она определяется как эталонная. При этом панорама окрашивается в темно-серый цвет. Запустив «СканАР» на выполнение, получают вторую (результирующую) панораму, имеющую уже три цвета: светло-серый — для участков спектра, на которых значения частот и уровней обоих панорам совпадают; темно-серый — для участков, на которых сигнал пропал, белый — появился новый (рис. 2.3.25).

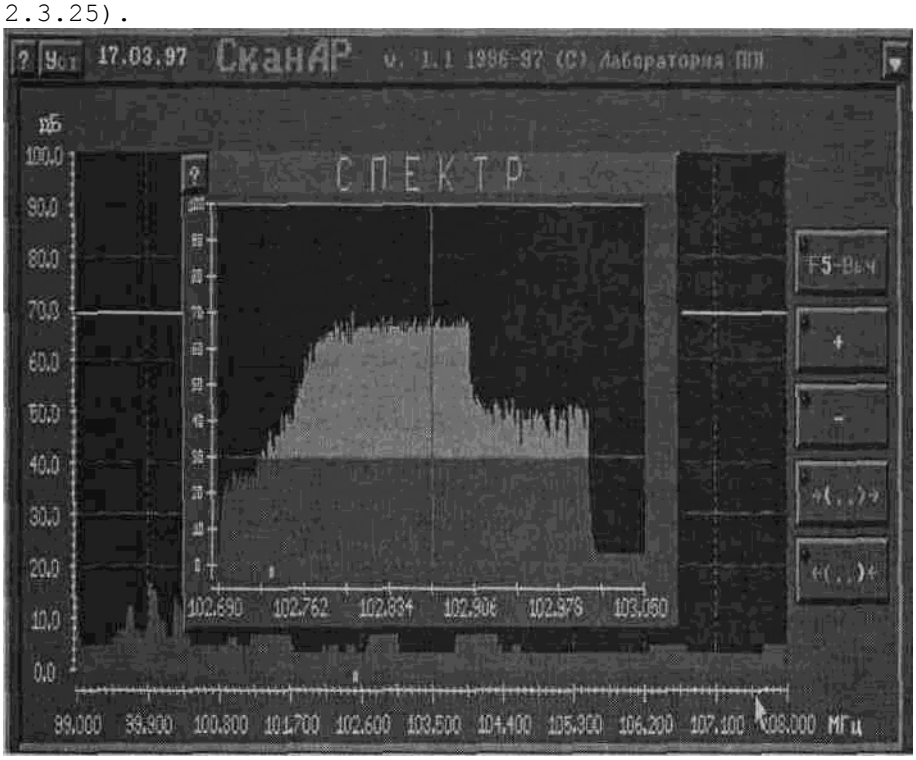



**Рис. 2.3.24. Фрагмент экрана при включенном подрежиме «Спектр»**

Чтобы извлечь панораму из архива, необходимо нажать клавишу F3 и в появившемся списке выбрать требуемую клавишей **Ok.** В противном случае нажать клавишу «Отменить».

**>•** Режим «Поиск» предназначен для наблюдения за изменением уровня сигнала в нескольких частотных диапазонах. Причем для каждого из них задаются свои параметры работы (шаг перестройки, вид модуляции принимаемого сигнала, значение аттенюатора и порогового уровня). Всего в программе предусмотрена возможность задания до 20 частотных диапазонов (в новой версии программы — до 120).

Для запуска «СканАРа» в режиме «Поиск» создается программа исполнения, которая может состоять из нескольких заданий. Создание задания подразумевает ввод значений левой и правой границ частотного диапазона и вышеперечисленных параметров — шага перестройки приемника, типа детектора, положения аттенюатора и величины порога.

Для создания программы служит таблица, появляющаяся после нажатия на кнопку **«Поиск»** (рис. 2.3.26). Каждая строка таблицы яв-

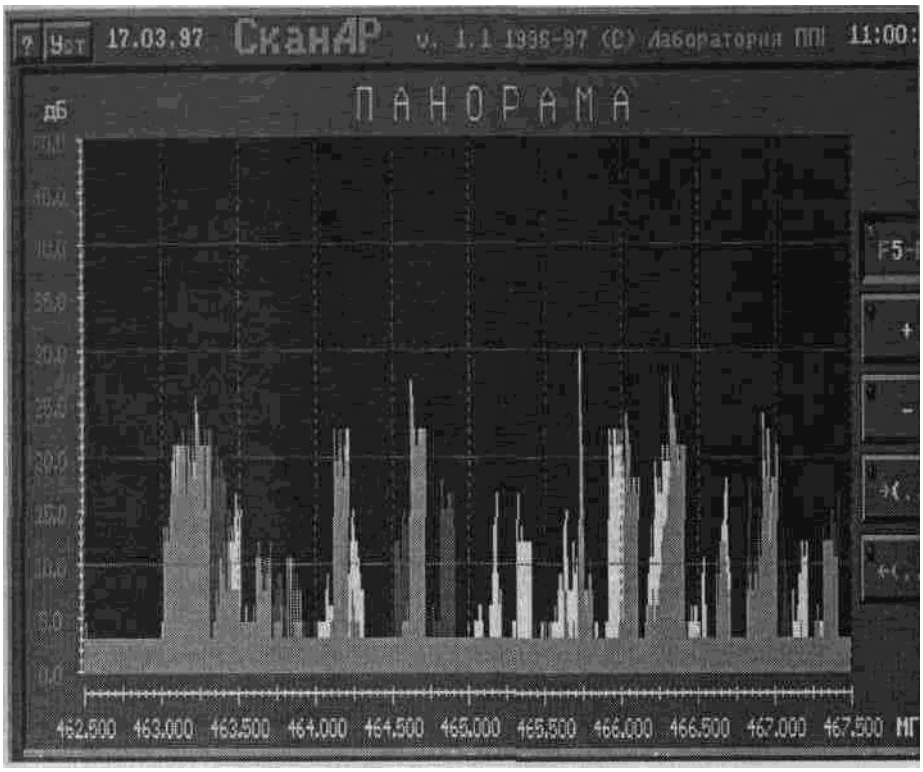
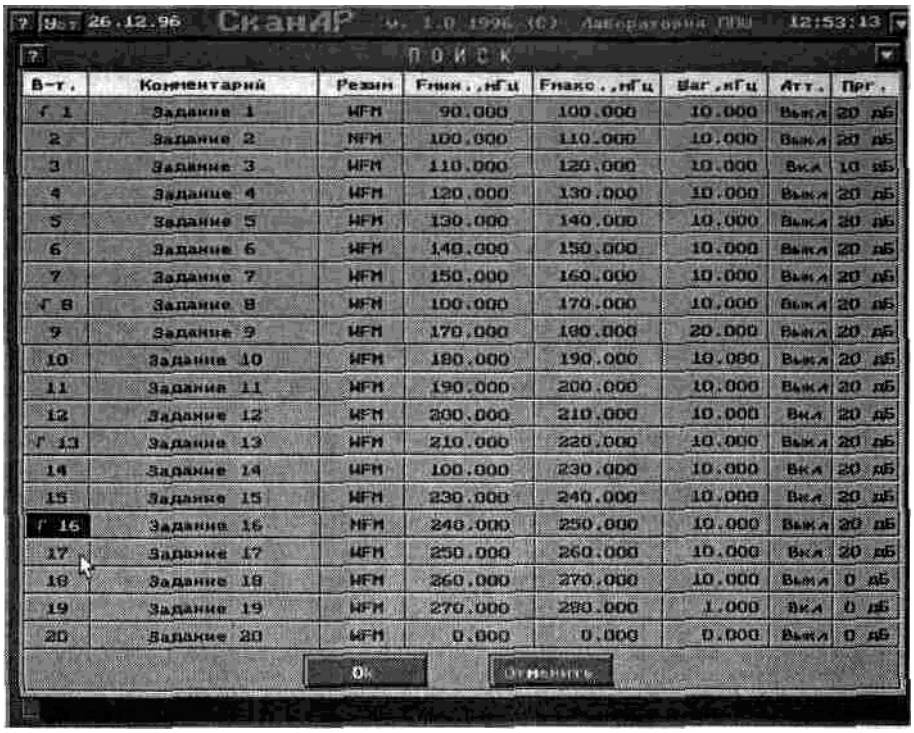



**Рис. 2.3.25. Подрежим «Сравнение панорам»**

ляется элементом программы и может быть включена в программу по желанию пользователя.

Первый столбец таблицы показывает номер задания и предназначен для отметки тех из них, которые будут включены в программу. Перемещение по столбцу осуществляется стрелками «↑» и «↓↓», а включение задания в программу — нажатием клавиш **«Пробел»** или «Insert». Для исключения из программы — повторным нажатием тех же **«Пробел»** или «Insert». Во второй колонке указывается комментарий для каждого задания. Он не влияет на работу программы и служит лишь для облегчения работы пользователя. Третий столбец предназначен для выбора вида модуляции анализируемых сигналов в каждом задании. Для выбора детектора используются клавиши **«Пробел»** или **«Insert»**, при этом появляется линейка с возможными вариантами. Нужный из них выбирается с помощью «горячей» клавиши и кнопки **«Enter»**.

Колонки «**Fмин**» и «**Fмакс**» предназначены для задания значений частот левой и правой границ диапазона. Для изменения значения используются




| N-т. | Комментарий | Режим | Fмин.,кГц | Fмакс.,кГц | Шаг,кГц | Атт. | Прг. |
|---|---|---|---|---|---|---|---|
| 1 | Задание 1 | WFM | 90.000 | 100.000 | 10.000 | Выкл | 20 дБ |
| 2 | Задание 2 | WFM | 100.000 | 110.000 | 10.000 | Выкл | 20 дБ |
| 3 | Задание 3 | WFM | 110.000 | 120.000 | 10.000 | Вкл | 10 дБ |
| 4 | Задание 4 | WFM | 120.000 | 130.000 | 10.000 | Выкл | 20 дБ |
| 5 | Задание 5 | WFM | 130.000 | 140.000 | 10.000 | Выкл | 20 дБ |
| 6 | Задание 6 | WFM | 140.000 | 150.000 | 10.000 | Выкл | 20 дБ |
| 7 | Задание 7 | WFM | 150.000 | 160.000 | 10.000 | Выкл | 20 дБ |
| 8 | Задание 8 | WFM | 100.000 | 170.000 | 10.000 | Выкл | 20 дБ |
| 9 | Задание 9 | WFM | 170.000 | 180.000 | 20.000 | Выкл | 20 дБ |
| 10 | Задание 10 | WFM | 180.000 | 190.000 | 10.000 | Выкл | 20 дБ |
| 11 | Задание 11 | WFM | 190.000 | 200.000 | 10.000 | Выкл | 20 дБ |
| 12 | Задание 12 | WFM | 200.000 | 210.000 | 10.000 | Вкл | 20 дБ |
| 13 | Задание 13 | WFM | 210.000 | 220.000 | 10.000 | Выкл | 20 дБ |
| 14 | Задание 14 | WFM | 100.000 | 230.000 | 10.000 | Вкл | 20 дБ |
| 15 | Задание 15 | WFM | 230.000 | 240.000 | 10.000 | Вкл | 20 дБ |
| 16 | Задание 16 | WFM | 240.000 | 250.000 | 10.000 | Выкл | 20 дБ |
| 17 | Задание 17 | WFM | 250.000 | 260.000 | 10.000 | Вкл | 20 дБ |
| 18 | Задание 18 | WFM | 260.000 | 270.000 | 10.000 | Выкл | 0 дБ |
| 19 | Задание 19 | WFM | 270.000 | 280.000 | 1.000 | Вкл | 0 дБ |
| 20 | Задание 20 | WFM | 0.000 | 0.000 | 0.000 | Выкл | 0 дБ |

**Рис. 2.3.26. Окно выбора и редактирования заданий в режиме «Поиск»**

те же **«Пробел»** или **«Insert»**, ввод нового значения осуществляется клавишей «Enter».

Кроме того, в каждом задании устанавливаются значение порога и положение аттенюатора, а шаг перестройки вычисляется автоматически в зависимости от заданных значений граничных частот диапазона.

Переход к выполнению программы происходит после нажатия клавиши «Enter» или кнопки **«Ok»**. Для выхода без сохранения изменений в программе и возврата в режим «Панорама» предназначена клавиша **«Отменить»**.

В режиме «Поиск» программа выводит окно, аналогичное окну режима «Панорама», но с выключенными кнопками изменения частоты, шага и порога.

После запуска программа сначала отработает первое задание, то есть пройдет первый заданный диапазон с определенным шагом и порогом, затем второе и т. д. После выполнения последнего задания программа снова перейдет к первому.

>• Режим «Обзор» предназначен для анализа широкого диапазона частот с отображением в виде зеленых точек сигналов, превышающих заданный порог.

В данном случае также предусмотрена возможность просмотра сигнала и спектра на интересующей частоте, сохранение полученной информации в архиве, вывод на принтер.

В случае остановки сканирования прием сигнала будет осуществляться на текущей, фиксированной частоте. При этом в окне «Частота и уровень» (рис. 2.3.27) отображаются значения, соответствующие положению курсора мыши или белого перекрестия, причем эти значения выводятся красным цветом, если уровень сигнала превышает установленный порог, зеленым — если нет.

При нажатии на кнопку **«Продолжить»** сканирование будет продолжаться с текущей частоты, а при нажатии кнопки **«Сначала»** сканирование начнется с начальной частоты диапазона.

При работе в режиме «Обзор» может возникнуть необходимость подробно просмотреть ряд сигналов, для этого используются подрежимы «Спектр», «Сигнал» или «Панорама обзора» (рис. 2.3.28). Полученные данные, как и

в режиме «Панорама», могут быть сохранены в архиве на жестком диске. Для извлечения данных из архива используется клавиша «**F3**».

>• Режим «Сканирование» предназначен для слежения за состоянием каналов выбранного банка памяти (аналогичен режиму сканирования банков памяти в приемнике). Результат сканирования отображается в виде зависимости время—уровень для каждой из 20 частот текущего банка (рис. 2.3.29). Комплекс позволяет наблюдать за состоянием 20 каналов текущего банка памяти с точностью от 1 до 12 с в течение 10 ч. Предусмотрена возможность задания 20 банков памяти по 20 каналов в каждом банке.

При остановке сканирования комплекс осуществляет прием сигнала на фиксированной частоте с возможностью перестройки приемника по заданным частотам банков памяти.

Для выбора банка памяти и значения сканируемых (контролируемых) частот в каждом банке служит кнопка **«Канал»**, после нажатия на которую появляется окно для выбора банка, назначения частот


**Рис. 2.3.27. Окно «Частота и уровень»**

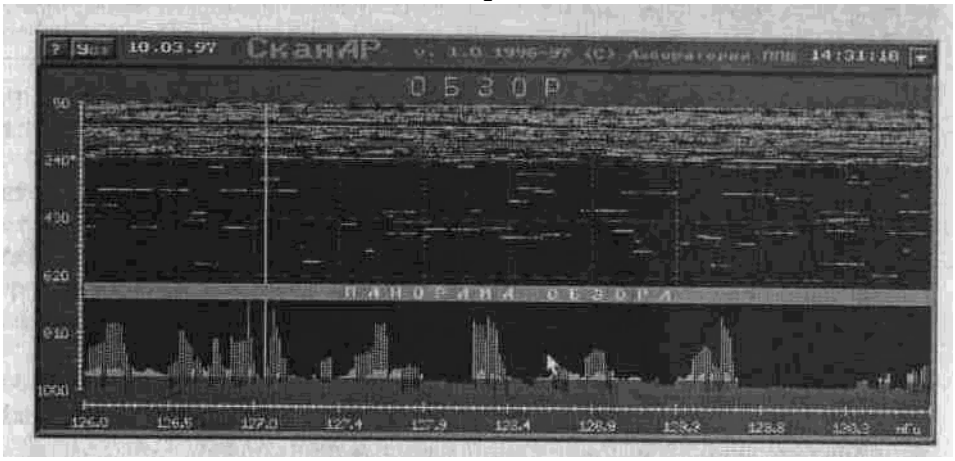



**Рис. 2.3.28. Фрагмент экрана при включенном подрежиме «Панорама обзора»**


**Рис. 2.3.29. Общий вид экрана в режиме «Сканирование»**

и других параметров сканирования. Для удобства пользователей все данные задаются в виде таблицы (рис. 2.3.30).

В первых двух колонках отображается номер банка памяти и комментарий для него, в качестве которого обычно используют условное обозначение, например название радиостанции, работающей на контролируемой частоте. В третьей колонке задается вид модуляции принимаемого сигнала. В поле «Частота», соответственно,— значение частоты, подлежащей контролю.

После запуска программа осуществляет сканирование по списку заранее заданных частот.

**Программы семейства Sedif.** В это семейство входят три программы: Sedif Plus, Sedif Pro и Sedif Scout, являющиеся, пожалуй, наиболее известными из всех подобных российских программ. Хотя в основном они реализуют примерно те же функции и возможности, что и другие рассматриваемые программы.

>• Sedif Plus — наиболее простой вариант, осуществляющий все основные необходимые функции программы.

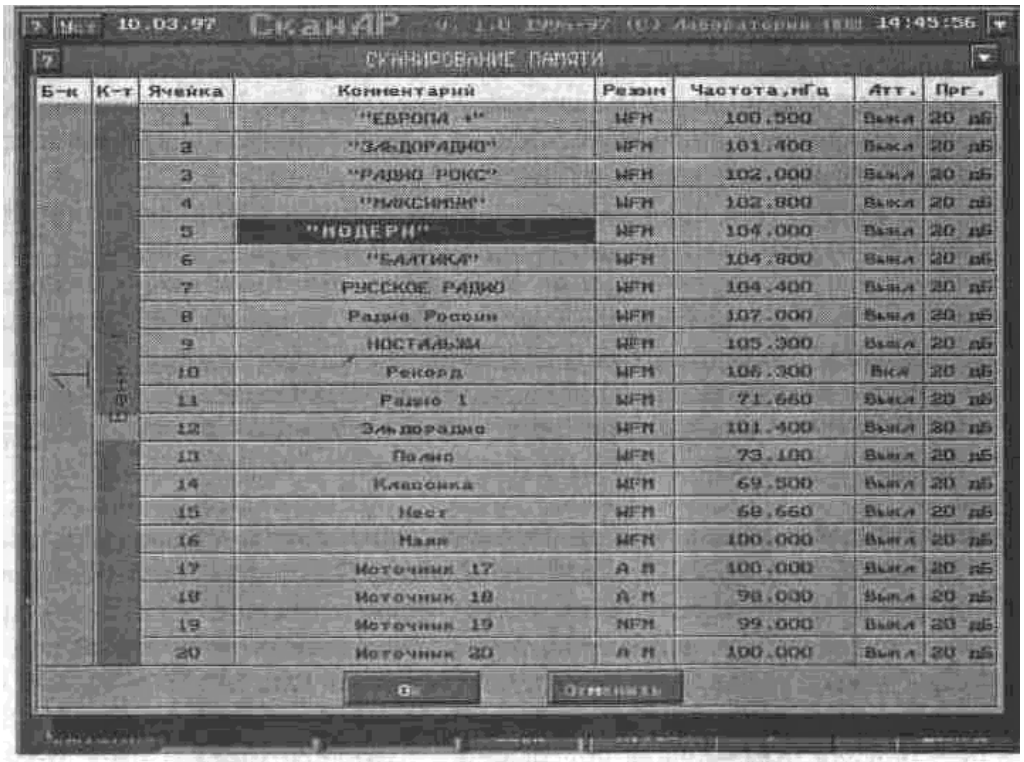



**Рис. 2.3.30. Окно выбора банка памяти и параметров сканирования**

>• Sedif Pro дополнительно позволяет работать со звуковыми картами типа Sound Blaster (однако необходима полная совместимость со стандартами фирмы Creative Labs). Эта возможность позволяет записывать принимаемые приемником сигналы на жесткий диск компьютера и в дальнейшем их анализировать и обрабатывать.

>• Sedif Scout имеет еще один дополнительный режим, названный «Поиск». В этом режиме возможно определение местоположения радиомикрофона, размещенного в том же помещении, что и приемник. Конечно, для удачной локализации необходимо соблюсти ряд условий, иначе вероятность может резко снизиться.

На сегодняшний день дальнейшее развитие продуктов серии Sedif остановлено. Его постепенно вытесняет новый программный продукт Filin.

**Программа Filin** может быть отнесена к примерам удачной реализации концепции функционального совмещения специального приемника с персональной ЭВМ.

Программа предназначена для работы в операционных системах Windows'3.1 или Windows'95 и позволяет использовать для поиска ЗУ следующие типы сканирующих приемников: AR-3000A, AR-2700, AR-8000, IC-R10, IC-R8500, а при наличии приставки-анализатора спектра SDU-5000 и радиоприемники IC-R7000, IC-R7100 и IC-R9000. Она обладает информативным интерфейсом (рис. 2.3.31), отображающим процесс работы аппаратуры поиска, характеристики сигналов и промежуточные результаты их анализа.

В программе предусмотрен набор корреляторов, позволяющих по тестовому акустическому сигналу или по естественному акустическому фону помещения опознавать принимаемый сигнал как излучение радиозакладки. Реализован ряд функций автоматического поиска неизвестных или подозрительных излучений. Кроме того, она дает возможность проводить анализ принимаемых сигналов по их спектрам, осциллограммам, корреляционным функциям и другим характеристикам.

**Программа RSPlus** удачно сочетает возможности поиска средств негласного съема информации и радиоконтроля. Одновременное отображение эталонной и

текущей панорам в расположенных друг под другом окнах при одновременной раскраске новых источников делает программу удобной для последовательного поиска в одном или нескольких помещениях.
Важная особенность программы — наличие банка частот, в котором могут храниться «портреты» источников: в число записывае-

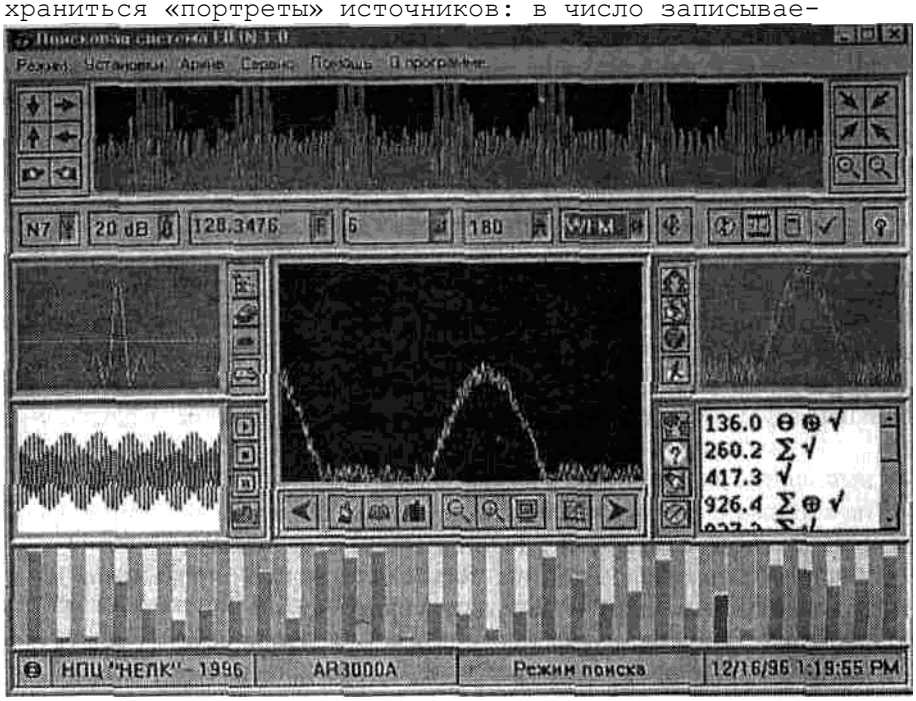



**Рис. 2.3.31. Экранная панель программы Filin**

мых характеристик включаются не только спектральные портреты для первых трех гармоник, но и их звуковые образы.
Однако в специальной литературе встречаются ссылки на наличие в программе множества недоработок.
**Программа «Крот-mini»** радикально отличается от предыдущих тем, что создана для работы в фоновом режиме операционной среды Windows'95 и принципиально ориентирована на пользователя, не обладающего специальными знаниями.
В программе реализован алгоритм анализа принимаемых излучений на принадлежность к сигналам радиозакладок, позволяющий последовательно переходить от поиска закладок с простыми типами модуляции к устройствам со всеми более экзотическими (и, следовательно, менее вероятными) способами маскирования и кодирования информации.
**Программа «ARCON»** работает под управлением операционной системы Windows'95, выполняя практически те же функции, что и рассмотренные выше программные продукты. Основное отличие состоит в том, что под каждый вид радиоприемного устройства (AR-3000, AR-8000, IC-8500 и т. д.) применяется свой пользовательский интерфейс, что позволяет максимально реализовать возможности и функции, присущие каждому сканеру.

### 2.3.4. Программно-аппаратные комплексы

Дальнейшим шагом по пути совершенствования процедуры поиска ЗУ является применение программно-аппаратных комплексов радиоконтроля и выявления каналов утечки информации, так как их возможности значительно шире, нежели чем у просто совмещенных с ЭВМ сканирующих приемников. В наиболее общем виде эти возможности заключаются в следующем:
>• выявление излучений радиозакладок;
**>•** пеленгование радиозакладных устройств в реальном масштабе времени;

>• определение дальности до источников излучения;
>• аналого-цифровая обработка сигналов с целью определения их принадлежности к излучению радиозакладок;
>• контроль силовых, телефонных, радиотрансляционных и других сетей;
>• работа в многоканальном режиме, позволяющем контролировать несколько объектов одновременно;
>• постановка прицельных помех на частотах излучения радиозакладок и др.

На рынке специальных технических средств защиты информации сегодня представлено достаточно изделий как отечественного, так и зарубежного производства, в той или иной степени реализующих эти функции. Однако поиск средств негласного съема информации и, в частности, локализация источников радиосигналов, находящихся в так называемой ближней зоне, остается их основным предназначением. Решение задачи поиска обеспечивается наличием в составе комплексов следующих элементов:

>• широкодиапазонного перестраиваемого по частоте приемника (сканера);
>• блока распознавания радиозакладок, осуществляющего идентификацию излучений радиомикрофонов на основе сравнения принятых про-детектированных сигналов с естественным акустическим фоном помещения (пассивный способ) или тестовым акустическим сигналом (активный способ);
>• блока акустической локации, позволяющего по запаздыванию переизлученного зондирующего звукового импульса определять расстояние до активных радиомикрофонов;
>• электронно-вычислительной машины (процессора), осуществляющей как обработку полученных данных, так и управление приемником.

По принципу построения все известные приборы данного класса делятся на две основные группы:

>• специально разработанные комплексы, конструктивно выполненные в виде единого устройства;
>• комплексы, сформированные на базе серийного сканера, персонального компьютера (обычно notebook) и специального программного обеспечения, аналогичного рассмотренному в п. 2.3.4.

Среди приборов первой группы наибольшей популярностью пользуются **OSC-5000 (Oscor), CPM-700** («Акула») и **ST 031 («Пиранья»).**

**OSC-5000 (Oskor)**

Его название происходит от Omni Spectral Correlator и характеризует основное назначение как спектрального коррелятора (рис. 2.3.32). Прибор разработан американской фирмой Research Electronics IntL, однако имеет сертификат Гостехкомиссии при Президенте РФ (сертификат № 81), что говорит о несомненных достоинствах прибора.

Программно-аппаратный комплекс Oscor достаточно хорошо известен и на российском, и на мировом рынке, ему более шести лет, и за эти годы он неоднократно модифицировался (с версии 1.6 до 2.2). Цена комплекса в зависимости от конфигурации колеблется от 12 000 до 16 000 $.

OSC-5000 представляет собой функциональное сочетание нескольких приборов.

Во-первых, это панорамный приемник последовательно-параллельного типа (сканер), перекрывающий диапазон частот 10 кГц...3 ГГц с полосой пропускания 15 кГц. Столь широкий диапазон перестройки обеспечивается наличием нескольких входов (фактически нескольких приемников), к каждому из которых подключена своя антенна (рамочная, штыревая и дискоконусная). Анализ может производиться как во всем диапазоне, так и в заданных полосах (до 31 полосы), автоматически или в ручном режиме. Максимальная скорость перестройки по частоте составляет 93 МГц/с при полосе пропускания 250 кГц. Чувствительность приемника соответствует значению 0,8 мкВ, а динамический диапазон входных сигналов составляет

90 дБ. Прибор оснащен набором детекторов, что дает возможность принимать сигналы с различным видом модуляции.
Несомненным достоинством является наличие инфракрасного детектора с областью спектральной чувствительности 0,85—1,07 мкм и специального

**Рис. 2.3.32. Многофункциональный спектральный коррелятор OSC-5000 (Oskor)**

адаптера, позволяющего вести контроль наличия излучений от сетевых закладок в диапазоне частот 10 кГц...5МГц в проводных линиях с напряжением до 300 В.
Во-вторых, это осциллограф и анализатор спектра, позволяющий наблюдать амплитудно-временные развертки демодулированных сигналов и их спектры с разрешением по частоте не хуже 50 Гц.
Режим работы прибора, позволяющий осуществлять панорамный анализ выбранного диапазона частот с заданным разрешением носит название Sweep. В этом режиме можно масштабировать выбранный спектральный диапазон и выделять интересующие сигналы. Особо здесь следует подчеркнуть наличие специальной функции отображения меток пиков сигналов, так называемая функция Display Peak Signal, которая позволяет сохранять на экране метки пиков ограниченных во времени сигналов. Метки при этом остаются и при следующем сканировании, что бывает, необходимо для поиска и распознавания излучений передатчиков (закладок), работающих с перестройкой по частоте.
Режим Analise дает возможность более детального излучения спектральных форм выбранных в Sweep-режиме сигналов и их временных характеристик.
В-третьих, это коррелятор, необходимый для идентификации сигналов ЗУ.
Принцип работы коррелятора заключается в том, что демодулированный низкочастотный сигнал сравнивается с акустическим фоном помещения. При этом на коррелятор одновременно подается для сравнения два низкочастотных сигнала: первый — демодулированный с выхода приемника, второй — аудиосигнал акустического фона помещения или сигнал телефонной линии. Роль источника аудиосигнала может выполнять либо обычный микрофон, либо линейный выход применяемого аудиовоспроизводящего

устройства: CD-плейера или магнитолы.
На основании результатов этого сравнения рассчитывается коэффициент корреляции и в зависимости от полученного значения каждому обнаруженному сигналу присваивается один из пяти уровней тревоги. При превышении этим уровнем заданного пользователем порогового значения срабатывает система оповещения — это мигание сообщения на экране, звуковой сигнал, запись на диктофон или печать характеристик (по выбору). Прибор фиксирует частоту, тип демодулятора, дату и время обнаружения тревожного сигнала, сохраняет все эти данные в базе данных или выводит на встроенный термоплоттер. Прибор можно запрограммировать так, что при обнаружении тревожного сигнала будет распечатан его спектр или произойдет запись передаваемой информации на диктофон. Переключение в режим Correlation осуществляется нажатием всего одной клавиши.
В программно-аппаратном комплексе OSC-5000 предусмотрен режим загрузки в память частот, излучения на которых прибор будет считать «дружественными» (Friendly Signals, например, сигналы теле- и радиовещательных станций) и не затрачивать время на анализ в автоматическом режиме. Всего Oscor может хранить информацию (дату и время обнаружения, частоту, тип демодулятора, полосу) о 7168 сигналах при штатной памяти 128 кБ или о 28 672 при расширенном до 512 кБ объеме памяти. Эта информация может редактироваться пользователем, протоколироваться самим прибором на термоплоттере или сбрасываться на ПЭВМ через COM-порт для дальнейшей обработки.
Дополнительными опциями для **Oscor** являются следующие:
**>•** OVM-5000 (Video Monitoring Option), реализованная в комплекте OSC-5000 Deluxe и предназначенная для анализа видеосигналов систем PAL/SECAM/NTSC при поиске видеопередатчиков;
>• OTL-5000 (Trangulate and Locate Option) — акустический локатор, предназначенный для определения местоположения активных радиомикрофонов;
>• OPC-5000 — специальное программное обеспечение для работы с базами данных сигналов OSCOR через COM-порт персональной ЭВМ, а также организации дистанционного контроля работы комплекса через модем.
**>• СРМ-700.** Зонд-монитор СРМ-700 — это универсальный прибор, предназначенный для поиска и обнаружения устройств скрытого съема информации, известен у нас в стране как комплекс «Акула» (рис. 2.3.33). Он предназначен для решения следующих задач:
1. обнаружения радиосигналов специальных технических средств скрытого перехвата конфиденциальной информации (радиомикрофонов, импульсных передатчиков, устройств дистанционного управления), работающих в диапазоне частот 50 кГц...3 ГГц;
2. обнаружения ЗУ, использующих токопроводящие линии для передачи информации в диапазоне частот 15 кГц...1 МГц;
3. выявления скрытоустановленных микрофонов с передачей информации по специально проложенным проводам, а также определения степени опасности утечки информации за счет акусто-электрического преобразования в телефонных аппаратах, радиотрансляционных и других приборах;
4. обнаружения скрытых видеокамер и диктофонов;
5. выявления инфракрасных источников излучения (ЗУ с инфракрасным каналом передачи информации);
6. обнаружения каналов утечки акустической информации.
Первые три задачи являются основными, поэтому в любой комплект СРМ-700 обязательно входят три соответствующих зонда.
**>•** Высокочастотный (радиочастотный) РЧ-зонд с областью спектральной чувствительности 50 кГц...3 ГГц.
Это активный прибор с собственным коэффициентом усиления 20 дБ, обеспечивающий пороговую чувствительность приемного устройства на

уровне — 85 дБ относительно 1 мВт и динамический диапазон входных сигналов 100 дБ. Он обеспечивает, например, обнаружение источника мощностью 1 мкВт и частотой излучения 150 МГц на дальности около 2 м.

>• Низкочастотный ОНЧ-зонд для контроля токопроводящих линий.

Его диапазон рабочих частот лежит в пределах от 15 кГц до 1 МГц, пороговая чувствительность — не хуже 60 дБ относительно 1 мВт. Максимальный уровень постоянного напряжения в тестируемых линиях не должен превышать 300 В, а переменного с частотой 60 Гц... 1500 В.

**Рис. 2.3.33. Универсальный прибор СРМ-700 («Акула»)**

>• Высокочувствительный усилитель для прослушивания электромагнитных сигналов звукового диапазона (100 Гц... 15 кГц), возникающих вблизи токопроводящих линий.

Он имеет систему автоматической регулировки усиления и обеспечивает прием сигналов, уровень которых может изменяться в пределах от 1,7 мкВ до 10 В (135 дБ). Один выход устройства предназначен для контроля принимаемых сигналов через наушники в реальном масштабе времени, другой — для записи на магнитофон. Уровни выходных сигналов, соответственно, имеют значения 5 В и 25 мВ.

Для решения задач 4—6 применяются дополнительные зонды:

>• электромагнитный зонд MLP-700 — для обнаружения скрытых видеокамер и диктофонов;

>• инфракрасный зонд IRP-700 — для обнаружения инфракрасных источников излучения;

>• акустический зонд ALP-700 — для обнаружения каналов утечки акустической информации.

Кроме вышеперечисленных основных функций комплекс позволяет решать следующие задачи:

>• работа в дежурном режиме («мониторинга опасности») — отслеживает электромагнитную обстановку в контролируемом помещении и подает соответствующий сигнал при обнаружении неизвестного устройства (звуковой с частотой 2,8 кГц или световой с частотой мигания 2 Гц);

>• обеспечение непрерывной записи всех принимаемых сигналов на любой стандартный магнитофон.

Для контроля уровней принимаемых сигналов в приборе реализован 18-

сегментный жидкокристаллический индикатор (в руководстве пользователя он может быть назван как дисплей или монитор).
Питание комплекса осуществляется от специального сетевого адаптера или никель-кадмиевого аккумулятора с напряжением 12 В.
Для предварительной проверки работоспособности аппаратуры в ее комплект дополнительно могут входить:
>• TTM-700 — тестовый радиопередатчик мощностью 0,7 мВт;
>• CCT-700 — тестовый передатчик с передачей сигнала по энергетической сети;
>• IRT-700 — тестовый инфракрасный передатчик.
Несомненно, комплекс CPM-700 («Акула») американской фирмы Research Electronics Intl. является достойным представителем рассматриваемого класса приборов.
**ST 031 («Пиранья»),** Российский комплекс по своим характеристикам практически не уступает вышеперечисленным приборам, а порой и опережает их, имея при этом малые размеры и вес (180x97x47 мм; 0,8 кг).
Он предназначен для проведения оперативных мероприятий по обнаружению и локализации технических средств негласного получения конфиденциальной информации, а также контроля естественных и искусственно созданных технических каналов утечки информации (рис. 2.3.34).
Фактически ST 031 — это комплекс, состоящий из следующих приборов:
>• высокочастотного детектора-частотомера;
>• сканирующего анализатора проводных линий;
>• детектора инфракрасных излучений;
>• детектора низкочастотных магнитных полей;
>• виброакустического приемника;
>• акустического приемника;
>• проводного акустического приемника.

**Рис. 2.3.34. Комплекс выявления технических каналов утечки информации ST 031 («Пиранья»)**

Важным достоинством «Пираньи» является то, что этот прибор позволяет анализировать принимаемые сигналы как в режиме осциллографа, так и в режиме анализатора спектра с индикацией численных параметров. При этом время вывода осциллограммы не превышает 0,2 с, а спектрограммы — 0,3 с. Разрешение собственного графического дисплея составляет 128x64 точки.

Чувствительность приемного устройства комплекса — 10 мВт, полоса пропускания — 22 кГц. Объем внутренней памяти позволяет удерживать от 15 до 60 отображений характеристик сигналов.

В табл. 2.3.5 представлены сравнительные характеристики основных функций и технических параметров многофункционального поискового прибора ST 031 («Пиранья») и ранее рассмотренного зонд-монитора СРМ-700 («Акула»). В качестве источников информации использовались технические паспорта на эти приборы.

Среди программно-аппаратных средств второй группы, созданных путем функционального объединения нескольких серийно выпускаемых устройств, на российском рынке активно предлагаются комплексы радиоконтроля и пеленгации ЗАО «Иркос».

**Таблица 2.3.5. Сравнительные характеристики поисковых комплексов СРМ-700 и ST 031**

| Функции | Характеристики | СРМ-700 («Акула») | ST 031 («Пиранья») |
|---|---|---|---|
| Высокочастотный детектор электромагнитного поля | Диапазон рабочих частот, МГц | 0,05-3000 | 30-2500 |
| | Чувствительность по входу, мВ: 1000 МГц 2000 МГц | 0,17 0,5 | 2 4 |
| Анализатор проводных линий | Диапазон частотомера, МГц | Отсутствует | 30...2400 |
| | Тип приемника | Широкополосный АМ-детектор | Перестраиваемый селективный приемник |
| | Вид демодуляции | АМ | АМ, FM |
| | Диапазон рабочих частот, кГц | 15...1000 | 10...15 000 |
| | Чувствительность по входу, мВ | 3 | 0,1 |
| | Максимальное напряжение, В | 300 | 600 |
| Звуковой усилитель | Диапазон рабочих частот, Гц | 100...15 000 | 150...20 000 |
| | Динамический диапазон, дБ | 135 | 80 |
| | Максимальное напряжение, В | 52 | 60 |
| Акустический приемник | Диапазон рабочих частот, Гц | Данные отсутствуют | 300...6000 |
| | Чувствительность, мВ/Па | | 5 |
| Виброакустический приемник | Диапазон рабочих частот, Гц | -"- | 300-6000 |
| | Чувствительность, В х $с^2$/м | | 1 |
| | Пороговая чувствительность, м/с | | 5 х$10^{-5}$ |
| Детектор ИК-излучения | Диапазон рабочих частот, Гц | м | 300-5000 |
| | Пороговая чувствительность, А/(мхГц$^{0,5}$) | | $10^{-6}$ |

Окончание табл. 2.3.5

| Функции | Характеристики | СРМ-700 («Акула») | ST 031 («Пиранья») |
|---|---|---|---|
| Детектор ИК-излучения | Спектральный диапазон, нм | -"- | 770-1000 |
| | Пороговая чувствительность, Вт/ $Гц^{0}$ | | $10^{-13}$ |
| | Диапазон рабочих частот, кГц | | 0,05-1000 |
| Осциллограф | Полоса пропускания, кГц | Отсутствует | 22 |
| | Чувствительность по входу, мВ | | 10 |
| | Погрешность измерений, % | | 1 |
| | Скорость вывода осциллограммы, с | | 0,2 |
| Спектроанализатор | Полоса пропускания, кГц | -"- | 22 |
| | Чувствительность по входу, мВ | | 10 |
| | Погрешность измерений, % | | 1 |
| | Скорость вывода спектрограммы, с | | 0,3 |
| Индикация | Акустическая | Встроенный громкоговоритель, головные телефоны | Встроенный громкоговоритель, головные телефоны |
| | Визуальная | 18-сегментный ЖК-индикатор | Графический ЖК-дисплей (128X64) |

**Комплексы АРК.** Они представлены семейством стационарных, мобильных (автомобильных, вертолетных) и портативных приборов.
С точки зрения поиска ЗУ наибольший интерес представляют именно

портативные комплексы **АРК-Д1 (КРОНА-1), АРК-ПК** и многоканальный комплекс контроля помещений учреждения **АРК-ДЗ** (КРОНА-2), рис. 2.3.35.
Эти приборы построены на базе сканирующего приемника AR-3000A, функциональные возможности которого расширены за счет специально разработанного синтезатора частот, процессора быстрого преобразования Фурье и 12-разрядного аналого-цифрового преобразователя. В результате этого обеспечена скорость перестройки 40—70 МГц/с в диапазоне частот 1...2000 МГц. Динамический диапазон входных сигналов лежит в пределах от 55 до 58 дБ.
Отличительными особенностями комплексов АРК являются следующие:

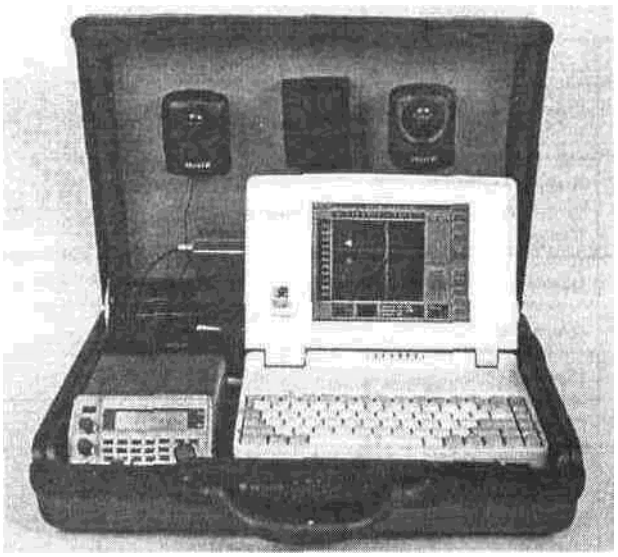


**Рис. 2.3.35. Портативный автоматизированный комплекс радиоконтроля АРК-Д1**

>• возможность обнаружения излучений радиомикрофонов, работающих под прикрытием мощных станций, различение внешних и внутренних источников излучений для контролируемых помещений.
Данная функция обеспечивается за счет применения разнесенной антенной системы, состоящей из 3—4 широкополосных антенн типа АРК-А1, АРК-А2, а также внешней опорной антенны АРК-А4 или АРК-А5М;
>• контроль наличия ЗУ в сетях переменного тока с напряжением до 400 В (с помощью устройства АРК-КПС), радиотрансляционных, телефонных и других сетей в диапазоне до 30 МГц;
>• контроль излучений внедренных портативных телевизионных камер (устройство АРК-КТВ);
>• активное и пассивное выявление излучений **специальных технических** средств негласного съема аудиоинформации.
Активный способ реализован на основе применения специально подобранных акустических зондирующих сигналов; пассивный — на использовании естественного акустического фона помещения, анализе гармоник излучений ЗУ, а также анализе сигналов с выхода опорной вынесенной из контролируемого помещения антенны. При этом обеспечивается надежная идентификация сигналов с амплитудной и частотной модуляцией, инверсией спектра и частотными перестановками («частотной мозаикой»).
>• Локализация мест размещения источников излучения в контролируемом помещении.
>• Подавление радиозакладных устройств путем создания прицельных по частоте помех с помощью малогабаритных передатчиков АРК-СПМ, которые могут быть размещены в нескольких контролируемых помещениях и дистанционно управляться многоканальным комплексом АРК-ДЗ.
Специально разработанный пакет прикладных программ СМО-Д5,

предназначенный для работы в среде Windows'95, обеспечивает следующие возможности:

**>•** управление всеми устройствами комплекса в одном пакете (режимы «Панорама», «Обнаружение», «Поиск», «Контроль ВЧ», «Контроль НЧ», «ТВ»);

**>•** изменение конфигураций используемых антенн;

>• использование любого из алгоритмов тестирования радиоизлучений на принадлежность к классу радиомикрофонов;

**>•** измерение уровней сигналов с выходов антенн (в децибеллах относительно 1 мкВ по входу радиоприемного устройства);

>• записи спектральных характеристик принимаемых излучений на жесткий диск персональной ЭВМ и их дальнейшей обработки.

Благодаря размещению в кейсе с универсальным питанием от сети переменного тока, автомобильной бортовой сети и автономных аккумуляторов комплексы **АРК-Д1 и АРК-ПК** могут быть использованы как для работы в помещениях, так и на выезде в сложных условиях эксплуатации.

Помимо рассмотренных, на рынке имеется достаточно широкий выбор и других приборов аналогичного назначения — это «Дельта-П», КРК-1, RS-1000, ECR-2, RANGER, Scanlock ECM+ и др.

Какому конкретно комплексу отдать предпочтение, зависит прежде всего от решаемых задач и возможностей потребителя.

Необходимо только помнить, что ни один прибор не сможет обеспечить для вас 100-процентную защиту от всех средств шпионажа. Кроме того, каждая система решает свои строго определенные задачи, а эффективность ее работы зависит главным образом от того, насколько профессионально она используется.

И последнее, хотя стоимость в гораздо большей степени отражает затраты и рыночную политику производителя или продавца, чем специальные характеристики приборов, все же надо иметь в виду, что работоспособная система, включающая в свой состав стандартный сканер или специальный приемник, не может стоить дешевле 800—1200 $, поэтому если вам предлагают панацею от всех бед за 200—300 $, то лучше воздержитесь от подобной покупки.

### 2.3.5. Нелинейные радиолокаторы

#### Общие сведения о нелинейных локаторах

Одной из наиболее сложных задач в области защиты информации является поиск внедренных ЗУ, не использующих радиоканал для передачи информации, а также радиозакладок, находящихся в пассивном (неизлучающем) состоянии. Традиционные средства выявления такие, как панорамные радиоприемники, анализаторы спектра или детекторы поля, в этом случае оказываются неэффективны. Визуальный осмотр также не гарантирует обнаружение подобных ЗУ, так как современные технологии позволяют изготовлять их с любым видом камуфляжа, прятать в элементах строительных конструкций и интерьера (п. 1.3).

Именно эта проблема и привела к появлению совершенно нового вида поискового прибора, получившего название нелинейного радиолокатора. Своим названием он обязан заложенному физическому принципу выявления подслушивающих устройств.

Дело в том, что технические средства промышленного шпионажа являются радиоэлектронными устройствами. В их состав входят полупроводниковые элементы (диоды, транзисторы, микросхемы), для которых характерен нелинейный вид вольт-амперной характеристики, связывающей протекающий через p—n-переход электрический ток i с приложенным напряжением и (рис. 2.3.36, а). Наличие такой нелинейной связи приводит к возникновению на выходе полупроводникового прибора бесконечно большого количества переменных напряжений (гармоник) с частотами fn = n x fo, где n = 1,2,3,.. (любое натуральное число), а fo— частота зондирующего сигнала,

действующего на входе полупроводникового прибора. Сам факт возникновения сигнала с частотой fo на входе полупроводникового элемента обязан явлению наведения ЭДС и токов в случайных антеннах, которыми могут оказаться проводники печатных плат или другие компоненты ЗУ при облучении их высокочастотным сигналом.

Таким образом, нелинейный локатор — это прибор, который просто реализует следующий принцип: излучает электромагнитную волну с частотой fo, а принимает переизлученные сигналы на частотах f^. Если такие сигналы будут обнаружены, то в зоне действия локатора есть полупроводниковые элементы, и их необходимо проверить на возможную принадлежность к ЗУ.

В соответствии с вышесказанным нелинейный радиолокатор обнаруживает только радиоэлектронную аппаратуру и, в отличие от классического линейного радиолокатора, «не видит» отражений от окружающих предметов, то есть обладает высокой избирательностью.

Источниками помех для его работы могут служить контакты со слабым прижимом, для которых характерно наличие промежуточного окисного


**Рис. 2.3.36. Вольт-амперные характеристики соединений, вызывающих появление высших гармоник в переизлученном сигнале:**

а — характеристика p-n-перехода полупроводникового прибора; б — характеристика случайного перехода «металл—окисел—металл»

слоя (сваленные вместе металлические канцелярские скрепки, монеты; плетеные сетки) или просто подвергнутые коррозии металлы. В редких случаях (при большой мощности излучения) нежелательный эффект могут дать паяные и сварные соединения.

Причина возникновения указанных помех связана с тем, что слабые металлические контакты, как правило, представляют собой квазинелинейные элементы с неустойчивым p—n-переходом, вызванным наличием окислов на поверхности металлов. В физике полупроводников подобные структуры известны как «металл — окисел — металл», а нелинейные элементы такого типа называются МОМ-структурами. Вольт-амперная характеристика случайного соединения, в отличие от характеристики p—n-перехода, обычно симметрична. Примерный вид ее показан на рис. 2.3.36, б. Методы селекции сигнала в нелинейных радиолокаторах на фоне подобных помех подробно будут рассмотрены ниже.

Впервые принципы нелинейной радиолокации были применены еще в середине 70-х годов, когда на контрольно-пропускных пунктах заводов и складов были установлены устройства предупреждения о попытке скрытного выноса радиоаппаратуры или ее электронных компонентов. После этого идеей заинтересовались спецслужбы и стали разрабатываться приборы обнаружения скрытых электронных средств разведки и радиовзрывателей.

Несмотря на свою специфичность принципы нелинейной локации нашли себе и мирное применение. Так, например, в настоящее время получили широкое распространение системы обнаружения несанкционированного

**Таблица 2.3.6. Основные характеристики современных нелинейных локаторов**

Наименование (страна-производитель) /Частота излучаемого сигнала, МГц /Мощность излучаемого сигнала, Вт /Вид излучения; параметры антенны /Номер принимаемой гармо- /Чувствительность приемника /Тип питания /Масса, кг /Примечания

1 /2 /3 /4 /5 /6 /7 /8 /9

// / / / / /18- полный комплект; /

Superscout-C 1 (США) /915 /0.3...2 /Непрерывный /2;3 /— /Сетевое и аккумуляторное /6,4— при питании от сети; 7,4— при питании от аккумулятора /

Superscout (США) /215 /0,016 ... 0,065 /Тоже /2,3 /- /Тоже /17,7-полный комплект /

Superscout (1995г., США) /915 /- /-"- /2;3 /- /Аккумуляторное /20- полный комплект /

Broom (Великобритания) /888,5 (для США - 915) /0,02...0,3; 0,06...0,9; регулируемая /-"- /2;3 /$10^{-15}$ Вт /Тоже /10,2-полный комплект; 7-без упаковки /Индикация уровня сигнала на ЖКИ. Антенна крепится на телескопической штанге 0,6...1,5м

Superbroom (Великобритания) /888,5 /Регулируемая /-"- /2;3 /- /Сетевое и аккумуляторное /- /Индикация уровня сигналов и их разности на ЖКИ. АМ-детектор 2-й и 3-й гармоник, FM-детектор. Приемник 2-й гармоники

Superbroom Plus (Великобритания) / /Тоже / /2; 3 /-120 дБ/Вт /Тоже /6,2-рабочий комплект /Индикация уровня сигналов 2-й и 3-й гармоник сигнала и их разности на ЖКИ;АМ-и FM- детекторы

Boomerang NGD-4 (NGD-5) (США) /915 /0,1(0,5) /Непрерывный; поляризация линейная, вертикальная и горизонтальная /2;3 /Глубина регулировки чувствительности -минус 30 дБ /Сетевое и аккумуляторное /17,5-полный комплект /Индикация уровня сигналов 2-й и 3-й гармоник

Locator PR (Великобритания) /888 /0,1 /Непрерывный; круговая поляризация /2 /- /Аккумуляторное /1,9 /Индикация уровня сигнала на ЖКИ; 210x180x60 мм

Searcher (Великобритания) /888 /850 мВт /То же /2 /- /Тоже /1,1 /Индикация уровня сигнала на ЖКИ. Антенна и основной блок объединены в одном корпусе; 220x75x55 мм

Продолжение табл. 2.3.6

Наименование (страна-производитель) /Частота излучаемого сигнала, МГц /Мощность излучаемого сигнала, Вт /Вид излучения; параметры антенны /Номер принимаемой гармоники /Чувствительность приемника /Тип питания /Масса, кг /Примечания

1 /2 /3 /4 /5 /6 /7 /8 /9

Orion NJE-4000 (США) /880...1000 /0,01...1 /-"- /2;3 /- /-"- /1,8 /Индикация уровня сигнала на ЖКИ. Антенна и основной блок крепятся на телескопической штанге. Инфракрасный наушник

РК 885-S (Германия) /- /- /- /- / /-"- /7,5 - без упаковки /

СОР 430 (Франция) /- /- /- /- / /-"-/5,8 - без упаковки /

Переход (Россия) /910 /0,4...0,в /Непрерывный /2 /$3x10^{-15}$ Вт; глубина регулировки чувствительности – минус 45 дБ /Сетевое и аккумуляторное /13 - полный комплект; 8 -без упаковки /450x320x140 ММ

Родник-ПМ (Россия) /910 /0,4...0,8 /Непрерывный » /2 /Глубина

регулировки чувствительности — минус 45 дБ /Сетевое и аккумуляторное /12 - полный комплект; 7-без упаковки /

Родник-2 (Россия) /910 /3 /Тоже /2 /-147 дБ/Вт; глубина регулировки чувствительности — минус 45 дБ /Тоже /4,9-рабочий комплект с аккумулятором /

Родник-23 (Россия) /910 /0.3...4 /Непрерывный; коэффициент усиления 3...8 дБ; поляризация линейная; диаграмма направленности главного лепестка 100° /2;3 /Тоже /М /15 — рабочий комплект /Индикация уровня сигналов 2-й и 3-й гармоник на ЖКИ

Энвис (Россия) /910 /0,04...0,4; 0,08...0,8; регулируемая /Непрерывный /2;3 /$3x10^{-15}$ Вт; глубина регулировки чувствительности – минус 45 дБ /-"- /15,5 -полный комплект; 8 -без упаковки /Индикация уровня сигналов 2-й и 3-й гармоник на ЖКИ

Обь-1 (Россия) /1000 /0,25 /Непрерывный; диаграмма направленности антенны 400 /2 /$3x10^{-15}$ Вт; глубина регулировки чувствительности - минус 60 дБ /-"- /6 /Индикация уровня сигналов 2-й и 3-й гармоник на ЖКИ; 200x140x90 мм; уровень зондирующего сигнала на стрелочном приборе

Лотос (Россия) /895 / /Импульсный /2 /$10^{-11}$ Вт /Сетевое /5-без упаковки /

Циклон-М (Россия) /680 /50-300; регулируемая (средняя мощность излучения -0,12)/Импульсный /2 /$3x10^{-12}$ Вт; глубина регулировки чувствительности – минус 30 дБ /Аккумуляторное и сетевое /2,5-без упаковки /170x120x40 мм

Окончание табл. 2.3.6

Наименование (страна-производитель) /Частота излучаемого сигнала, МГц /Мощность излучаемого сигнала, Вт /Вид излучения; параметры антенны /Номер принимаемой гармоники /Чувствительность приемника /Тип питания /Масса, кг /Примечания

1 /2 /3 /4 /5 /б /7 /8 /9

Циклон-М1А (Россия) /680 /300 Вт; регулируемая (средняя мощность излучения -0,09) /Импульсный коэффициент усиления 3...8 дБ; поляризация линейная; диаграмма направленности главного лепестка — 100° /2 /-110дБ/Вт /Тоже /1,2 /150x120x40 мм

Октава (Россия) /890; частота следования импульсов -300...500 Гц, 15...25 кГц; длительность импульса —3 икс /20-300; 90-900; регулируемая /Импульсный /2 /$10^{-11}$ Вт; глубина регулировки чувствительности - минус 30 дБ /-"- /13 - полный комплект; 5-без упаковки /

Октава-М (Россия) /Тоже /25-400 /Тоже /- 2 /$3x10^{-11}$ Вт /-"- /9-комплект /160x150x50 мм

Люкс (Россия) /435; частота следования импульсов-1 кГц; длительность импульса -20 икс /0,14-14 /Импульсный /2 /1 мкВ; глубина регулировки чувствительности — минус 40 дБ /- / /-

Онега-2 (Россия) /900 /5 /Тоже /2 /Глубина регулировки чувствительности — минус 30 дБ /- /6,5 /

Онега-2М (Россия) /910 /100, средняя 0,08 /Импульсный; поляризация эллиптическая, суммарный коэффициент эллиптичности — 4 дБ /2 /-120 дБ/Вт; глубина регулировки чувствительности — минус 42 дБ /Аккумуляторное и сетевое /2,5-приемо-передающего блока с аккумулятором; 0,8-антенны со штангой /Блок приемопередатчика 206x145x65 мм; штатная упаковка 500x350x130; светодиодные линейные индикаторы, динамик, телефон

Онега-3 (Россия) /910; частота следования импульсов 400 Гц; длительность импульса - 5 мкс /100; средняя 0,24 /Импульсный; коэффициент усиления —3 дБ; поляризация эллиптическая; диаграмма направленности главного лепестка —90" /2,3 /-120дБ/Вт /Аккумуляторное t

/2 /Блок приемопередатчика 206х145х65 мм; кейс 500х350х130 ММ

Онега-3М (Россия) /910 /100; средняя 0,08 /Импульсный; поляризация эллиптическая, суммарный коэффициент эллиптичности —4 дБ /2,3 /-120 дБ/Вт по 2-й гармонике; - 115 дБ/Вт по 3-й гармонике; глубина регулировки чувствительности - минус 42 дБ /Аккумуляторное и сетевое /2,5-приемо-пе-редающего блока с аккумулятором; 0,8 -антенны со штангой /Блок приемопередатчика 206х145х65 мм; штатная упаковка 500х350х130; светодиодные линейные индикаторы, динамик, телефон

NR-900P (Россия) /900; частота следования импульсов -300 Гц, 6 кГц; длительность импульса -2 икс; 20 мкс /25-150 /Импульсный; коэффициент усиления —3 дБ; поляризация круговая; диаграмма направленности главного лепестка - 60-70° /2 /-115дБ/Вт; глубина регулировки чувствительности - минус 50 дБ /Тоже /штатной упаковке /Уровень 2-й гармоники переизлученного сигнала на ЖКИ; 165х70х190 мм

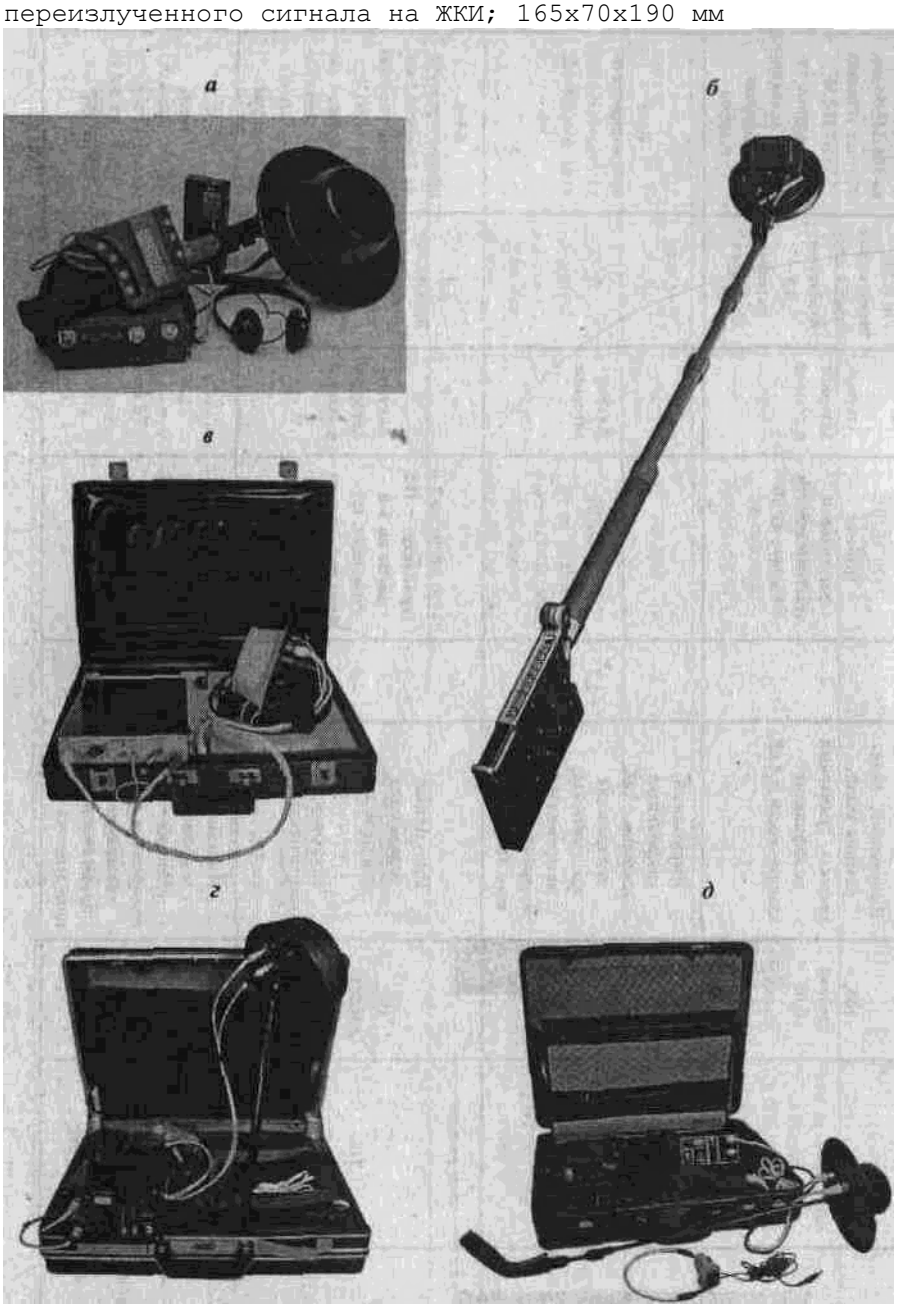


**Рис. 2.3.37. Нелинейные радиолокаторы:**
а — NR-900E; б — Orion; в — Октава, г — Обь; д — Онега-2М;

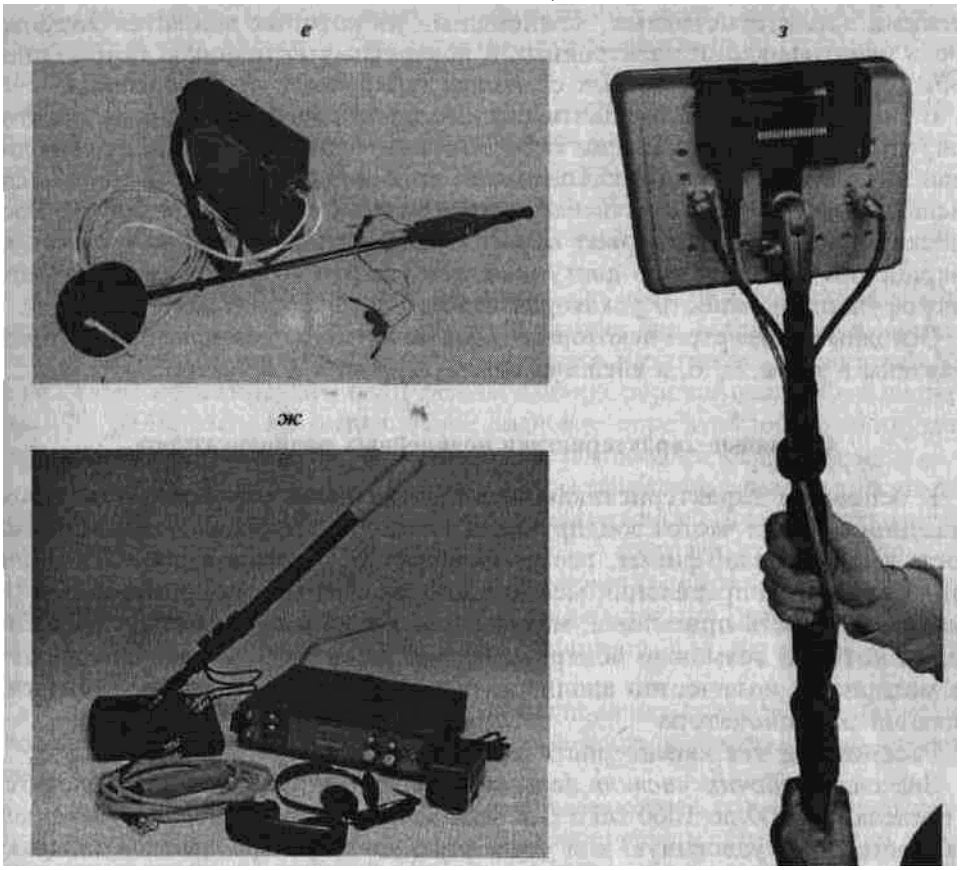



**Рис. 2.3.37. Окончание**
е — Родник-2М; ж — Broom ECM; з — Boomerang

выноса предметов из магазинов, поиск людей в снежных завалах и разрушенных зданиях, контроль багажа авиапассажиров и т. д.

Первым устройством, поступившим на вооружение спецслужб, в частности ЦРУ, был локатор Superscout, серийный выпуск которого начался с 1980 года. В 1981 году появился британский Broom, который несколько уступал американскому аналогу. Наш отечественный серийный локатор появился в 1982 году и назывался «Орхидея». Правда, раньше ему предшествовали несколько уникальных образцов, но они были сняты с появлением «Орхидеи».

В настоящее время на российском рынке представлено около двух десятков типов нелинейных радиолокаторов. Как правило, это портативные приборы отечественного и импортного производства стоимостью от 2000 до 30 000 $. Имеющий место разброс цен обусловлен различными техническими характеристиками, важнейшими из которых являются возможность идентификации электронных и контактных источников помех, способы индикации принимаемых сигналов, габариты, вес, тип питания.

В России производится почти столько же моделей нелинейных локаторов, сколько в США и Англии вместе взятых. Однако западные производители предлагают многофункциональные приборы с широким набором сервисных функций, что естественно влияет на цену (25 000—30 000 $). Российские производители держат качество приборов на должном уровне при сохранении относительно доступных цен (2000—10 000 $), за счет чего многофункциональность локаторов отходит на второй план.

Основные параметры некоторых типов нелинейных радиолокаторов

представлены в табл. 2.3.6, а внешний вид — на рис. 2.3.37.

**Основные характеристики нелинейных радиолокаторов**

К основным характеристикам нелинейных радиолокаторов относятся:
значения рабочих частот зондирующих сигналов; режим излучения и мощность передатчика; форма, геометрические размеры и поляризация антенн; точность определения местоположения переизлучающего объекта;
чувствительность приемника; максимальная дальность действия и глубина, на которой возможно обнаружение закладки внутри радиопрозрачного материала; количество анализируемых гармоник; размеры, вес и тип питания радиолокатора.

Рассмотрим эти характеристики более подробно.

Значения рабочих частот передатчиков всех типов локаторов находятся в пределах от 400 до 1000 МГц (рабочие частоты приемников, соответственно, составляют удвоенную или утроенную частоту передатчиков). Однако большинство отечественных и зарубежных образцов работают в диапазоне, близком к 900 МГц. Такой выбор обусловлен компромиссом в решении следующего противоречия:

>• с одной стороны, чем ниже частота зондирующего излучения, тем лучше его проникающая способность внутрь предметов и сред, в которых могут быть спрятаны ЗУ, и больше относительный уровень высших гармоник в переизлученном сигнале;

**>•** с другой — чем выше частота излучения, тем уже диаграмма направленности антенны локатора при фиксированных геометрических размерах, следовательно выше плотность потока мощности зондирующего сигнала (кроме того, на высоких частотах лучшими свойствами обладают случайные антенны, в качестве которых выступают ножки навесных элементов, проводники печатных плат и т. п., а их размеры, как известно, невелики).

К сожалению, многие нелинейные радиолокаторы функционируют на фиксированных частотах без возможности перестройки. Причина такого подхода — упрощение схемотехнических решений, то есть существенное снижение цены. Расплачиваться за такое упрощение приходится худшими эксплуатационными характеристиками, так как на частотах приема могут присутствовать излучения посторонних радиоэлектронных средств. И если даже уровни мешающих сигналов невелики, их может быть достаточно для нарушения нормальной работы радиолокаторов, так как чувствительность приемных устройств очень велика.

Естественно, более удобны в эксплуатации локаторы, имеющие возможность перестройки в определенном диапазоне. Так, например, в нелинейном локаторе Orion (NJE-400) фирмы Research Electronics International (REI) предусмотрен автоматический режим выбора рабочей частоты в диапазоне 880...1000 Мгц. Ее оптимальное значение определяется по наилучшим условиям приема для 2-й гармоники частоты зондирующего сигнала.

От рабочей частоты зависит форма и геометрические размеры антенн, важной характеристикой которых является поляризация. Передающие антенны имеют, как правило, линейную, а приемные — круговую поляризацию.

Точность определения местонахождения радиоэлектронного устройства, которую позволяют достигать используемые размеры антенн, соответствует нескольким сантиметрам. Например, для локаторов «Родник» и «Циклон» это 2 см.

Следующей группой характеристик нелинейных локаторов являются режим работы передатчика, излучаемая мощность и чувствительность приемника.

В зависимости от режима работы нелинейные локаторы делятся на локаторы с непрерывным и импульсным излучением. Практически все зарубежные приборы и некоторые отечественные работают с непрерывными зондирующими сигналами малой мощности (10...850 мВт). Большинство отечественных локаторов работают в импульсном режиме излучения с пиковой мощностью

5...400 Вт. Из-за простоты используемых приемных устройств импульсные локаторы значительно дешевле непрерывных.

Следует отметить, что высокая мощность и характер излучения импульсных локаторов могут создать определенные проблемы в плане электромагнитной совместимости со средствами связи, навигации, телевещания, датчиками пожарной и охранной сигнализации и т. д. Кроме того, зондирующее излучение оказывает негативное воздействие на операторов, эксплуатирующих аппаратуру. Поэтому, в соответствии с санитарными нормами, мощность современных локаторов ограничена максимальным значением 3...5 Вт для непрерывного режима и средним значением 0,1...1,5 Вт (до 400 Вт в импульсе) — для импульсного. Однако даже при таких ограничениях у оператора после часа работы часто начинают болеть глаза, так как именно они наиболее чувствительны к СВЧ-излучению.

Некоторые современные нелинейные локаторы имеют возможность изменения мощности зондирующего сигнала. Так, в локаторе NJE-400 уровень непрерывного излучения регулируется в пределах от 0,01 до1 Вт, а в радиолокаторе «Циклон-М» пиковое значение импульсной мощности — от 80 до 250 Вт. Более того, приемник локатора Superbroom Plus снабжен функцией автоматического установления мощности излучения в зависимости от величины принимаемого сигнала на 2-й гармонике.

Чувствительность приемников современных нелинейных локаторов лежит в пределах от $10^{-15}$ до $10^{-11}$ Вт. У импульсных она несколько хуже, что объясняется соответствующим превосходством пиковой мощности импульсных передатчиков (примерно на 35—40 дБ). В большинстве радиолокаторов используются приемники с регулируемой чувствительностью. Диапазон регулировки этого параметра составляет 30...50 дБ.

В соответствии с законом сохранения энергии (чем выше номер принимаемой гармоники n, тем меньше ее амплитуда) в современных локаторах анализируются только 2-я и 3-я гармоники зондирующего сигнала. И тем не менее, нелинейные радиолокаторы являются приборами ближнего действия, так как коэффициент преобразования энергии облучающего сигнала в энергию высших гармоник очень мал. Конкретная дальность действия зависит от множества факторов. В первую очередь, это тип обнаруживаемого устройства, наличие у него антенны и ее длина, условия размещения объекта поиска (в мебели, за преградами из дерева, кирпича, бетона и т. п.).

Максимальное расстояние, на котором возможно выявление ЗУ ограничено величиной 0,5 м. Данное значение соответствует варианту работы на открытых площадях или в больших необорудованных помещениях, например таких, как готовящийся к сдаче строительный объект. Для офисных помещений возможности обнаружения еще скромнее. Это связано с высокой концентрацией различных помеховых объектов (канцелярские принадлежности, оргтехника и т. п.).

С понятием максимальной дальности действия тесно связана максимальная глубина обнаружения объектов в маскирующей среде. Для строительных конструкций она может достигать несколько десятков сантиметров. Например, локаторы серии «Циклон» обнаруживают радиоэлектронные изделия в железобетонных стенах толщиной до 50 см, в кирпичных и деревянных — до 7 см.

Важной характеристикой является и количество анализируемых гармоник переизлученного сигнала. Так как одновременный прием на двух гармониках зондирующего сигнала дает неоспоримые преимущества по сравнению с однотональным приемом: он дает возможность осуществлять идентификацию обнаруженных объектов.

Современные нелинейные локаторы имеют небольшие размеры, вес и позволяют работать как от электросети, так и от автономных источников питания (аккумуляторов).

Например, у нелинейного локатора «Омега» вес приемопередающего блока составляет 2 кг, а антенны со штангой — 0,8 кг. Вес нелинейного локатора «Циклон-М» в упаковке (кейсе) — 5,5 кг (при этом вес приемопередающего блока составляет 1,2 кг). У нелинейного локатора Orion (NJE-400) приемопередающий блок и антенна закреплены на одной телескопической штанге, и общий вес конструкции не превышает 1,8 кг. Для удобства работы в этом локаторе используются беспроводные инфракрасные наушники.

Конструктивное исполнение изделий «Переход», «Родник-ПМ» и «Энвис» дает оператору возможность работать без постоянного перемещения приемопередающего блока аппаратуры, который размещен в чемодане типа «атташе-кейс». Блок соединен с антенным датчиком кабелем длиной 5—7 м. Узел управления и индикации аппаратуры (регулировка мощности и чувствительности, световые индикаторы, гнездо головных телефонов) размещен на антенном датчике.

Иногда нелинейные локаторы выполняются в ранцевом варианте.

**Способы селекции помех от случайных источников**

Среди основных способов селекции сигнала на фоне помеховых воздействий, вызванных наличием в обследуемом пространстве случайных преобразователей частоты зондирующего излучения, выделяют следующие:

>• по относительному значению уровней принимаемого излучения на 2-й и 3-й гармониках частоты сигнала;

>• по характеру изменения амплитуды шума на выходе приемника вблизи переизлучающего объекта;

>• по реакции объекта на вибровоздействия;

>• по наличию информационных признаков в принимаемом сигнале.

1. Этот способ применим для локаторов, снабженных функцией приема на двух гармониках частоты зондирующего сигнала (приборы Superbroom, Superscout, «Энвис» и др.). Он основан на различии преобразующих свойств полупроводниковых элементов и случайных МОМ-структур.

Физическая сущность способа заключается в том, что для полупроводниковых элементов характерен более высокий уровень переизлученного сигнала на 2-й гармонике по сравнению с 3-й (примерно на 20—40 дБ), и наоборот, контактные источники помех переизлучают сигнал на 3-й гармонике с большим уровнем, чем на 2-й.

Для удобства операторов такие нелинейные локаторы снабжены двумя индикаторами, относительная степень свечения которых и свидетельствует об амплитуде сигналов в соответствующих каналах (рис. 2.3.38). Индикаторные устройства могут располагаться непосредственно на приемопередающем

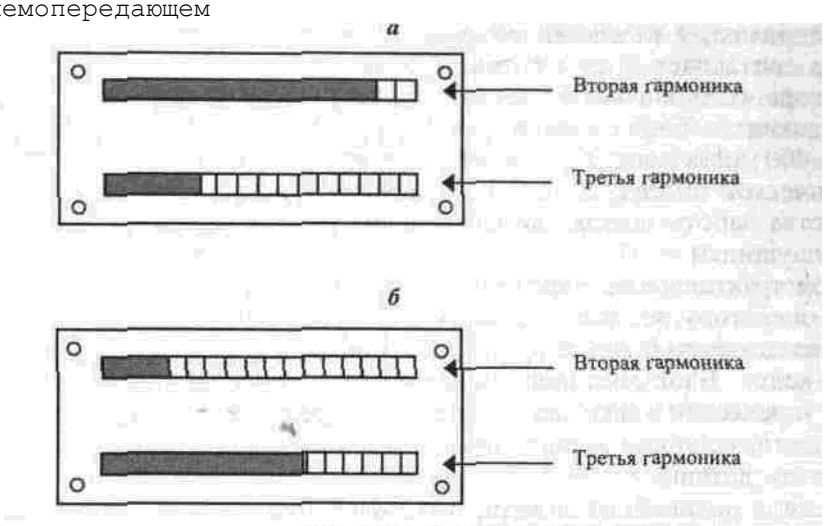


**Рис. 2.3.38. Способ селекции помех по относительному уровню 2-й и 3-й гармоник переизлученного сигнала:**
а — обнаружен полупроводниковый элемент; б — в зоне облучения присутствует контактный источник помех блоке (локаторы Superbroom, «Омега-3») или на антенной штанге (локаторы NJE-400, NR-900E, «Энвис»).
2. Характер изменения амплитуды шума на выходе приемника локатора также может служить признаком наличия объекта с нелинейной вольт-амперной характеристикой.
Так, при приближении антенны локатора к месту расположения полупроводникового элемента в головных телефонах, подключенных к выходу приемника, наблюдается значительное понижение уровня шума (примерно на 8—10 дБ). Минимальное значение Uш имеет место на расстоянии DR от лоцируемого объекта, не превышающем 5 см (кривая 2, рис. 2.3.39).
И наоборот, уменьшение расстояния между антенной и случайной МОМ-структурой сопровождается некоторым возрастанием уровня шума (кривая 7).
К сожалению, применение данного способа может быть несколько ограничено следующими двумя факторами:
>• данный способ может быть реализован только в локаторах, оснащенных амплитудным детектором;
>• некоторые типы случайных электрических контактов вызывают не увеличение, а уменьшение амплитуды шума на выходе приемника радиолокатора.

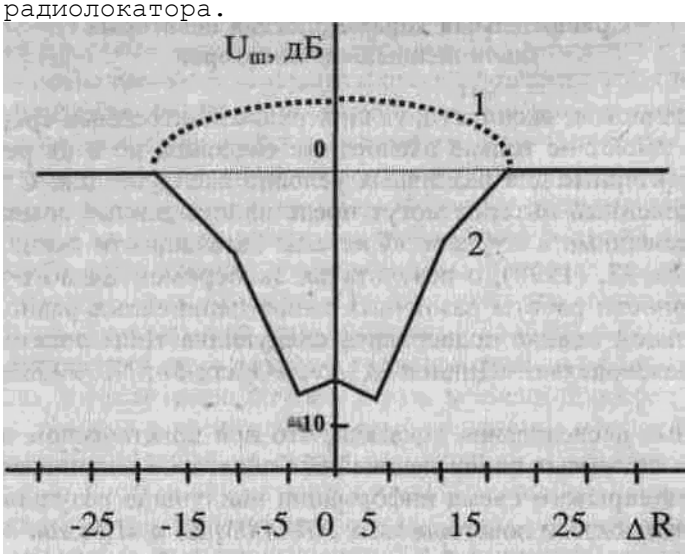



**Рис. 2.3.39. Способ селекции помех по характеру изменения относительного уровня шума на выходе приемника нелинейного локатора:**
1 — наличие помехового объекта; 2 — полупроводниковый элемент
3. Весьма эффективным способом селекции истинных полупроводниковых объектов на фоне ложных является физическое воздействие на исследуемый участок, например, методом простукивания. Характер звука в головных телефонах при этом позволяет судить о типе переизлучающего объекта: в случае ложного соединения в наушниках возникает типичное потрескивание на фоне тонального сигнала; в случае полупроводникового элемента сигнал остается чистым.
При использовании локаторов, работающих на двух гармониках, анализ объекта методом простукивания сопровождается наличием дополнительной информации о случайном объекте: хаотичным изменением уровня на световых индикаторах.
Часто в набор инструментов нелинейного локатора входит специальный резиновый молоток, предназначенный для простукивания поверхностей, под

которыми могут быть спрятаны ЗУ.
4. Ряд отечественных локаторов («Переход», «Родник-ПМ» и «Энвис») обеспечивают дополнительный способ анализа принятого от объекта сигнального отклика, а именно прослушивание процессов, происходящих в активно функционирующем объекте. Так, могут быть прослушаны речь, передаваемая подслушивающим устройством, тон таймера электронного взрывателя и т. п. Принцип получения этого эффекта аналогичен процессу модуляции при высокочастотном навязывании. Последний режим распознавания обеспечивает практически 100-процентную идентификацию объекта.

**Сравнительная характеристика некоторых типов нелинейных локаторов**

Для специалистов, эксплуатирующих радиоэлектронные средства, важное значение имеют не только паспортные сведения, но и их реальные параметры, характерные для различных условий эксплуатации. С этой точки зрения определенный интерес могут представлять данные компании «Гротек», опубликованные в журнале «Системы безопасности связи и телекоммуникаций» № 23, (1998), о результатах экспериментального исследования эффективности работы различных типов нелинейных радиолокаторов.

Сравнительной оценке подверглись следующие типы локаторов отечественного производства: «Циклон-MlA»; «Онега-3»; NR-900M; NR-900E; «Родник-23».

Проведенные исследования показали, что при практическом использовании вышеперечисленных типов нелинейных локаторов для поиска электронных устройств скрытого съема информации наилучшие результаты показали мощные импульсные локаторы типа NR-900M(E) и «Циклон-MlA», которые во многих случаях не требуют двустороннего обследования массивных элементов интерьера, обязательного вскрытия подвесных потолков, плинтусов и обеспечивают уверенный поиск в толще строительных конструкций.

Тем не менее, при их использовании глубина односторонней «просветки» не должна превышать 20—25 см, в противном случае потребуется увеличение мощности передатчика или чувствительности приемника локатора, что приведет к росту количества ложных срабатываний, увеличению времени анализа или даже к пропуску объекта. Поэтому правильный подбор оператором чувствительности и мощности приборов нелинейной локации при обследовании различных мест проверяемого помещения имеет большое значение.

Следует отметить, что локаторы серии NR самые универсальные и удобные в эксплуатации приборы. Они имеют хорошую чувствительность и избирательность, а также вполне современный внешний вид. При правильной настройке элементов управления позволяют легко отстраиваться от помеховых воздействий. Это самые чувствительные к экранированным закладкам локаторы. Узкая диаграмма направленности главного лепестка антенной системы и хорошее подавление задних ее лепестков позволяют эффективно работать рядом с бытовой оргтехникой без выноса их из помещений.

При умелом использовании нелинейный радиолокатор «Родник-23» также способен эффективно выявлять электронные устройства несанкционированного съема информации. Это удобный в эксплуатации и самый чувствительный прибор, поэтому работа в помещениях с большим количеством электронной техники затруднена из-за срабатываний локатора на помеховые объекты. При работе с этим устройством рекомендуется, по возможности, выносить или переставлять электронику от обследуемых мест. Глубина односторонней «просветки» не должна превышать 10—15 см. Это, естественно, увеличивает время проверки массивных элементов интерьера, но зато вероятность пропуска минимальна. «Родник-23» в режиме с

выключенной модуляцией позволяет прослушивать сигнал отклика от электронных объектов, находящихся во включенном состоянии, при приеме излучения на 2-й гармонике зондирующего сигнала (например, при облучении работающего радиомикрофона отлично прослушивается акустика помещения). В ходе испытаний было отмечено, что локатор не оказывает вредного влияния на организм человека и не создает помех для работающей бытовой и другой техники, что также можно отнести к несомненным достоинствам прибора.

Основной недостаток «Родника-23» заключается в использовании антенны с линейной поляризацией, что приводит к необходимости обследования любой поверхности в двух взаимно перпендикулярных направлениях и, соответственно, к увеличению почти в 2 раза времени проверки помещения.

Самые скромные результаты продемонстрировал нелинейный радиолокатор «Онега-3», который по своим техническим и эксплуатационным характеристикам несколько уступил остальным исследованным приборам. Основной и существенный его недостаток — отключение звукового тона в головных телефонах при превышении 3-й гармоникой зондирующего сигнала уровня 2-й. Это существенно затрудняет обнаружение и даже приводит к возможному пропуску закладки, находящейся рядом с помеховым объектом, например, рассыпанной мелочью, проволокой и т. п. Таким образом, сфера применения нелинейного локатора «Онега-3» ограничивается поиском в поверхностном слое строительных конструкций и элементах интерьера. Он способен обнаружить только простейшие объекты, серьезно не экранированные и не имеющие специальных фильтров, снижающих эффективную нелинейную поверхность рассеивания искомого объекта.

Сравнительная оценка значений максимальной дальности обнаружения различных типов ЗУ для указанных видов нелинейных локаторов приведена в табл. 2.3.7.

**Основные выводы**

1. Нелинейные локаторы полностью не решают задачу выявления закладок в помещении. Так, например, если закладка с дистанционным управлением установлена в какой-либо электронной аппаратуре (телевизоре, телефонном аппарате и т. п.) и включается только во время проведения совещания, то она не может быть обнаружена нелинейным локатором при обследовании помещения перед переговорами, так как сигнал отклика от нее будет замаскирован откликом от аппаратуры, в которой она вмонтирована. Поэтому в комплекте с локатором всегда должен использоваться панорамный приемник того или иного типа. При этом весьма желательно, чтобы контроль несанкционированных излучений в помещении осуществлялся и во время совещаний.

**Таблица 2.3.7. Максимальная дальность обнаружения электронных устройств (Rmax, м)**

Тип тестового устройства /Тип нелинейного локатора /«Цикяон-М1А» /«Онега- 3» /NR-900M /NR-900E /«Родник-23»

Контрольное устройство аппарата NR-900E /0.5 /0,8 /0,8 /0,7 /1.1

Радиомикрофон, 50x28x10 мм, длина антенны La= 17 мм, несущая частота f=418 МГц, корпус металлический /1,6 /1,9 /19 /1,15 /2,5

Радиомикрофон, 28x18x11 мм, La=77 мм, f=105,7 МГц, металлический /1 /1,9 /1,9 /1,05 /1,9

Радиомикрофон, 31x9x8 мм, La=16 мм, J=410 МГц, металлический /0,7 /0,8 /0,8 /0,8 /1,1

Телефонный радиомикрофон-конденсатор, f=101 МГц, металлический /0,8 /1 /1 /1,3 /3,1

Телефонный радиомикрофон-конденсатор, 20x14x10 мм, f=93 МГц, пластмасса /1,5 /1,6 /8 /1 /3,8

Радиомикрофон, 58х35х18 мм, La=35мм, f=179,19 МГц, пластмасса/2 /2,5 /2,5 /1,8 /3,4

Радиомикрофон-бочонок, d= 18 мм, h=27 мм, La=57 мм, пластмасса /0,7 /1,1 /1,1 /0,44 /1,1

Радиостетоскоп, 60х40х20 мм, La=49 мм, f=108 МГц, пластмасса/1,6 /2 /2 /1,25 /3,1

2. При выборе нелинейного радиолокатора следует исходить из задач, поставленных перед группой контроля.

При работе на открытых пространствах целесообразно использовать импульсные локаторы большой мощности и наилучшей чувствительности. Это же относится и к обследованию в необорудованных помещениях, имеющих толстые стены.

При работе в офисах предпочтительно применять локаторы непрерывного излучения, в особенности те, которые позволяют контролировать процессы, происходящие в обнаруживаемых устройствах. Они не создают проблем по части электромагнитной совместимости и экологически безвредны. Среди непрерывных локаторов целесообразно использовать те, которые осуществляют прием сигнала одновременно на 2-й и 3-й гармониках, так как они значительно снижают нагрузку на оператора, сокращают время, требуемое на обследование, и позволяют избежать демонтажа строительных конструкций (что иногда необходимо при использовании локаторов, работающих на 2-й гармонике). Однако их цена почти вдвое выше, чем у локаторов, принимающих только на 2-ю гармонику.

3. Ряд ЗУ выполняется по МОП-технологии в экранированных корпусах. Поэтому их обнаружение даже с использованием нелинейных локаторов затруднено, так как уровень переизлученных сигналов на 2-й и 3-й гармониках незначителен. Для поиска таких ЗУ могут использоваться металлоискатели (металлодетекторы).

**2.3.6. Некоторые рекомендации по поиску устройств негласного съема информации**

Всю процедуру поиска можно условно разбить на несколько этапов:

>• подготовительный этап;

>• физический поиск и визуальный осмотр;

>• обнаружение радиозакладных устройств;

>• выявление технических средств с передачей информации по токоведущим линиям;

>• обнаружение ЗУ с передачей информации по ИК-каналу;

>• проверка наличия акустических каналов утечки информации.

**Подготовительный этап**

Предназначен для определения глубины поиска, а также формирования перечня и порядка проводимых мероприятий. Он включает в себя следующие элементы:

1. Оценку возможного уровня используемых технических средств.

Объем проводимых мероприятий существенным образом зависит от того, в чьих интересах они проводятся. Одно дело — проверка помещений представителей малого бизнеса, другое — крупнейших корпораций или государственных учреждений, так как при этом значительно отличается уровень выявляемых устройств, который может колебаться от примитивных радиомикрофонов до специальной профессиональной техники, и, соответственно, меняется уровень привлекаемой поисковой техники.

2. Анализ степени опасности, исходящей от своих сотрудников и представителей соседних организаций.

Хороший способ проверки — организация контролируемой утечки информации. Это может быть сделано посредством «случайного» присутствия постороннего человека, «забытого» документа или другим доступным

способом.
3. Оценку возможности доступа посторонних в помещения.
4. Изучение истории здания, в котором планируется проводить поисковые мероприятия.
Оценивается возможность установки закладок как во время строительства, так и оставления их в наследство от предыдущих обитателей.
5. Определение уровня поддерживаемой безопасности в соответствии с экономическими возможностями и степенью желания заказчика, а также фактической необходимостью.
6. Выработку плана действий, который должен отвечать следующим условиям:
**>•** время поиска должно приходиться на рабочие часы, когда ЗУ активны;
**>•** должны быть созданы условия, провоцирующее к действию возможно внедренные «жучки», поскольку в них могут быть использованы как схемы VOX, включающие устройства только при определенном уровне акустического сигнала, так и системы дистанционного управления (проведение фиктивных, но правдоподобных деловых переговоров — хороший повод, чтобы побудить противоположную сторону активизировать свои устройства);
>• должна быть обеспечена скрытность проводимых мероприятий — если есть необходимость ведения своей «контрразведывательной» игры, то следует помнить, что разговоры с коллегами и заказчиком, приход, развертывание аппаратуры, характерный шум поиска раскрывают содержание и результат проводимых мероприятий;
>• неожиданность — поиск следует проводить регулярно, но через случайные промежутки времени.

**Физический поиск и визуальный осмотр**

Физический поиск и визуальный осмотр является важным элементом выявления средств негласного съема информации (см. п. 2.3.1), особенно таких, как проводные и волоконно-оптические микрофоны, пассивные и полуактивные радиозакладные устройства, дистанционно управляемые «ждущие» устройства и другие технические средства, которые невозможно обнаружить с помощью обычной аппаратуры.
ПОМНИТЕ: физический поиск является базой для любой поисковой методики. Будьте предельно внимательны, смотрите тщательно!
Проведение поисковых мероприятий следует начинать с подготовки помещения, подлежащего проверке.
1. Необходимо закрыть все окна и, занавески для исключения визуального контакта.
2. Включить свет и все обычные офисные устройства, характерные для данного помещения.
3. Включить источник «известного звука» (тестового акустического сигнала) в центре зоны контроля. Во время поиска он будет выполнять важные функции:
>• маскировать большинство шумов, производимых во время физического поиска;
>• работать как источник для звуковой обратной связи, необходимой для выявления радиомикрофонов;
>• активизировать устройства, оснащенные системой VOX.
Источник «известного звука» не должен настораживать противоположную сторону, следовательно это может быть любой кассетный или CD-плейер. Необходимо только помнить, что лучшие результаты достигаются при использовании аппаратуры средних размеров. Это объясняется оптимальными размерами громкоговорителя. Выберите наиболее уместную в данной ситуации запись, будь то музыка, бизнес-семинар или курс самообучения. Подберите соответствующую длительность, поскольку качественный поиск может занять много часов.
Примечание: в качестве источника «известного звука» не рекомендуется

использовать радиоприемник, поскольку эту же станцию может поймать и ваша поисковая аппаратура, что может привести к ошибке и радиостанция будет зафиксирована как нелегальный радиопередатчик.
4. За пределами зоны контроля (в незащищенной комнате/зоне) как можно более бесшумно разверните вашу аппаратуру.
Незащищенная зона — это место, которое не вызывает интереса у противоположной стороны и не контролируется ею, поэтому ваши действия останутся скрытыми.
5. Установите обычный уровень радиоизлучения окружающей среды перед поиском в зоне контроля.
Основные процедуры поиска. Визуально, а также с помощью средств видеонаблюдения и металлодетекторов, обследуйте все предметы в зоне контроля, размеры которых достаточно велики для того, чтобы можно было разместить в них технические средства негласного съема информации. Тщательно осмотрите и вскройте, в случае необходимости, все настольные приборы, рамы картин, телефоны, цветочные горшки, книги, питаемые от сети устройства (компьютеры, ксероксы, радиоприемники и т. д.).
Для поиска скрытой проводки обследуйте плинтуса и поднимите ковровые покрытия. Тщательно осмотрите потолочные панели, а также все устройства, содержащие микрофоны, магнитофоны и камеры.
С особой тщательностью обследуйте места, где ведутся наиболее важные переговоры (обычно это стол с телефоном). Большинство нелегальных устройств располагаются в радиусе 7 м от этого места для обеспечения наилучшей слышимости и(или) видимости.
Если вы при этом используете нелинейный радиолокатор, то скрупулезно выполняйте требования его инструкции на эксплуатацию и рекомендации, изложенные в п. 2.3.5.
Особо следует обратить внимание на проверку телефонных линий, сетей пожарной и охранной сигнализации.
Следует обязательно разобрать телефонный аппарат, розетки и датчики и искать детали, непохожие на обычные с разноцветными проводами и спешной или неаккуратной установкой.
Затем осмотрите линию от аппарата (датчика) до стены и, удалив стенную панель, проверьте, нет ли за ней нестандартных деталей.
Проведите физический поиск в коммутационных панелях и коммуникационных каналах, в случае необходимости используйте эндоскопические и портативные телевизионные средства видеонаблюдения, описанные в п. 2.3.1. Проверьте места входа/выхода проводов внутри и снаружи здания.
С целью облегчения последующих поисковых мероприятий после завершения всех работ скрытно пометьте шурупы на стенных панелях, сетевых розетках, телефонных корпусах и других местах, куда могут быть установлены закладки. Тогда при проведении повторных проверок видимые в ультрафиолетовых лучах метки покажут нарушение целостности ранее обследованного объекта, если оно имело место, а соответствующие записи в вашем журнале проверок помогут сориентироваться в будущей работе. Для контроля изменений в окружающих устройствах очень удобны ультрафиолетовые маркеры.
При проведении поиска ЗУ в автомобиле тщательно осмотрите не только салон, но и раму автомашины, багажник и т. п., внимательно проверьте цепи, имеющие выход на автомобильную антенну. При проведении этих операций досмотровые портативные телевизионные системы также могут оказаться очень полезны.

**Обнаружение радиозакладных устройств**

Процедура поиска начинается с формирования опорной панорамы, которая представляет из себя совокупность частот и амплитуд легальных источников (их амплитудных спектров). Она может строиться как в ручную, так и автоматически, так как практически все современные программно-

аппаратные комплексы оснащены этой функцией. Частотная область, в которой будет осуществляться поиск радиозакладок ограничивается практически только возможностями применяемых приемников, но должна как минимум перекрывать диапазон 50... 1000 МГц. Раздвигать эти границы шире, чем от 300 кГц до 10 000 МГц вряд ли целесообразно.
Однако надо помнить, что применение опорной панорамы может послужить и причиной серьезных ошибок, приводящих в конечном итоге к пропуску излучения радиозакладок. Поэтому при использовании априорной информации о загрузке эфира необходимо учитывать следующие факторы:
>• опорная панорама должна строится на расстоянии от проверяемого помещения, существенно превышающем оперативную дальность приема излучения закладки (то есть на удалении не менее 2—3 км от контролируемого объекта), что позволит избежать ситуации, когда мощное ЗУ будет принято за легальный источник;
>• существует целая серия ЗУ, специально маскируемых под вещательные станции или устройства сотовой связи и работающих с небольшой отстройкой от них по частоте.
В качестве примерной последовательности производимых действий по выявлению радиозакладок можно порекомендовать следующий порядок.
1. Разместите прибор в центре контролируемого помещения, установите антенну, оденьте наушники.
2. Установите регулировки в такое положение, чтобы индикаторный прибор показывал среднее значение.
3. Выключите все приборы и свет в зоне контроля и близ нее и посмотрите, не изменились ли показания индикатора. Иногда обычная флуоресцентная лампа создает очень сильное радиоизлучение, в таком случае она должна быть выключена или удалена из комнаты. Если изменения в показаниях индикатора не могут быть вызваны такими явными причинами, то это означает реальное подозрение на «жучок».
4. Повращайте антенну в вертикальной и (или) горизонтальной плоскости (в зависимости от ее вида). Следите за показаниями индикатора, они будут меняться в зависимости от положения антенны.
5. Выделите направление с максимальным уровнем подозрительного излучения.
Идентификацию подозрительного сигнала как излучения радиозакладки проводите в соответствии с возможностями вашей аппаратуры. Это может быть:
>• прием переизлученного «известного звука» (тестового сигнала);
>•изменение в опорной панораме;
>• наличие большого уровня гармоник;
>• резкое изменение уровня при перемещении антенны и т. п. (см. при знаки излучений радиозакладок в п. 2.3.2).
6. Обследуйте все объекты, в которых могут быть спрятаны радиозакладки, например, с помощью индикатора поля, сканирующего приемника, программно-аппаратного комплекса.
Примечание: иногда обнаруживается ложный источник сигнала, «висящий» где-то в воздухе — это значит, что реальный источник рядом. Продолжайте поиск.
7. После обнаружения сигнала радиозакладки следует локализовать зону с повышенным уровнем этого излучения, отслеживая его по индикатору. Для этой процедуры применяется «ходьба по кругу», которая позволяет очертить «горячую» зону.
Нельзя прерывать режим скрытности после обнаружения «жучка», так как ЗУ может быть несколько. Это делается для улучшения качества приема и резервирования. Если противоположная сторона знает о ваших подозрениях на прослушивание, то она может специально поставить одну или несколько легко обнаруживаемых закладок, чтобы убедить вас в успехе проведенного

поиска и прекратить дальнейшие усилия. Если закладка оснащена приемником сигналов дистанционного управления, то нарушение режима скрытности приведет к немедленному отключению устройства, а следовательно, к усложнению поиска и, возможно, снижению его эффективности.

Примечание: в некоторых случаях увеличение уровня принимаемого подозрительного сигнала связано с приближением не к истинному, а к мнимому источнику, что может быть следствием, например, явления интерференции; характерным признаком излучений скрытоустановленных телевизионных камер является изменение характеристик принимаемого сигнала при изменении уровня освещенности (включения/выключения света в помещении).

Проверка элементов телефонных линий на наличие излучений радиозакладок, как правило, осуществляется по изменению уровня сигнала на входе приемника контроля в момент поднятия трубки. Если в линии установлена радиозакладное устройство, то процесс поднятия трубки сопровождается существенным изменением уровня принимаемого излучения, кроме того в наушниках прослушивается тональный сигнал номеронабирателя либо другой тестовый сигнал. В «чистой» линии имеет место только кратковременный скачок излучения в момент поднятия трубки (в наушниках слышен короткий щелчок), а тональный набор не прослушивается.

Для обеспечения благоприятных условий проверки целесообразно антенну приемника контроля держать как можно ближе к элементам телефонной сети — проводу, аппарату, трубке, распределительной коробке и т. д., последовательно перемещая ее от одной точки контроля к другой.

Однако не всегда наличие теста в радиосигнале свидетельствует о работе подслушивающих устройств. Вполне возможно, что причиной являются и паразитные электромагнитные излучения (ПЭМИ) самого телефонного аппарата, связанные с эффектом самовозбуждения его усилительных каскадов. Для выявления физической природы обнаруженных излучений целесообразно использовать приемные устройства с частотным диапазоном 10 кГц... 30 МГц, так как именно в нем сосредоточена наибольшая мощность ПЭМИ. При этом необходимо контролировать не только электрическую, но и магнитную составляющую поля. Для этого могут быть использованы специальные электрические (например, HE 010, HE 013/015, HFH 2Z1), магнитные (HFH 2-Z3, HFH 2-Z2) или комбинированные (FMA-11) антенны.

Наличие радиозакладных устройств с непосредственным подключением к телефонной линии эффективно можно обнаруживать и с использованием стандартных анализаторов телефонных линий. Единственное неудобство — необходимость предварительного обесточивания проверяемой линии.

В автомобиле наряду с обычными радиомикрофонами могут быть установлены и так называемые бамперные жучки — специальные технические средства для слежения за перемещением автомобиля с выходной мощностью 100 мВт... 5 Вт в импульсном режиме.

Поэтому выявление возможно внедренных устройств должно начинаться с их активизации. С этой целью необходимо:

разместить в салоне источник «известного звука» (тестового, сигнала), так как оба вида ЗУ могут быть снабжены системами VOX;

воссоздать условия, соответствующие реальной эксплуатации — автомобиль нужно завести, разогнать, затормозить и т. д.

И тогда по изменению уровня фона на удалении нескольких метров от транспортного средства можно сделать вывод о наличии ЗУ.

**Выявление технических средств с передачей информации по токоведущим линиям**

Осуществляется с использованием специальных адаптеров, позволяющих подключаться к различным линиям, в том числе и находящихся под

напряжением до 300—400 В.
Поиск необходимо производить в частотном диапазоне 50... 300 кГц. Это обусловлено, как отмечалось в п. 1.3.2, тем, что, с одной стороны, на частотах ниже 50 кГц в сетях электропитания относительно высок уровень помех от бытовой техники и промышленного оборудования, а с другой — на частотах выше 300 кГц существенно затухание сигнала в линии, и, кроме того, провода начинают работать как антенны, излучающие сигнал в окружающее пространство, поэтому устройства с частотами передачи 300 кГц и выше будут выявлены на этапе поиска радиозакладок.
К сожалению, некоторое оборудование, питаемое от сети, может производить характерный низкочастотный шум, который может быть принят за искомый сигнал «жучка», поэтому необходимо по очереди отключать все питаемые устройства, чтобы определить источник такого шума.
Примечание: регуляторы освещенности и дефектные флуоресцентные лампы также могут давать низкочастотный шум, который может быть устранен удалением такой лампы или выставлением регулятора на максимум. Применение полосового фильтра звукового диапазона также поможет уменьшить уровень шума. Однако простое выключение шумящей цепи недопустимо, так как этим можно выключить и закладное устройство!

**Обнаружение ЗУ с передачей информации по ИК-каналу**

Использование ИК-канала является хотя и экзотичным, но все же достаточно реальным способом передачи информации от ЗУ, поэтому исключать его применения нельзя.
Источником излучения является ИК- или лазерный диоды с узким пучком. Размещаются они либо напротив оконных проемов внутри контролируемых помещений, либо на наружной стороне зданий.
Наиболее надежный способ их выявления — физический поиск. Если же последний ничего не дал, то нужно использовать поисковую технику со специальными ИК-датчиками. Поиск излучений от таких ЗУ лучше всего осуществлять с наружной стороны здания. Особое внимание при этом уделяется окнам.

**Проверка наличия акустических каналов утечки информации**

Иногда ответственные за безопасность так поглощены поиском хитроумных жучков, что упускают из вида такие каналы утечки, как элементарное подслушивание за стеной. Звук может распространяться наружу через окна, стены, водопроводные трубы, полости в здании и т. д. и улавливаться микрофонами за пределами охраняемого помещения. Поэтому при проведении физического поиска обязательно проверяются вентиляционные и кабельные каналы на возможность прослушивания, а также на наличие в них вынесенных микрофонов, соединенных проводами со звукозаписывающей аппаратурой. В случае необходимости проводится полная акустическая проверка контролируемого помещения.

## 2.4. Технические средства защиты информации в помещениях и сетях связи

### 2.4.1. Общие принципы защиты

Среди всего многообразия способов несанкционированного перехвата информации особое место занимает прослушивание телефонных разговоров, поскольку телефонная линия — самый удобный источник связи между абонентами в реальном масштабе времени, и при этом самый незащищенный. Действительно, электрические сигналы сейчас, как и сто лет назад, продолжают распространяться по проводам в открытом виде. Как видно из материалов первой части книги, прослушать телефонную линию является

простым и дешевым делом. На основании печального опыта можно уверенно заявить, что если злоумышленники приняли решение о «разработке» объекта, то первое, что они сделают, это начнут контролировать телефонные переговоры своей потенциальной жертвы. Телефонная связь имеет еще один недостаток (с точки зрения безопасности) — открывает возможность перехвата речевой информации из помещений, по которым проходит телефонная линия, даже тогда, когда аппарат находится в «отбое». Впрочем, для таких целей годятся и другие проводные линии. Эта тема, пожалуй, наиболее часто эксплуатируется как авторами детективов, так и популярных изданий по безопасности, которые не скупятся на «ужасающие» подробности.

Специально для любителей такого рода литературы изложение этого материала начнем с небольшой цитаты из американской книги «Шпионаж особого рода»: «Питер Карлоу был техническим экспертом ЦРУ, и ему были известны признаки того, что телефон прослушивается. Сигнал после набора номера поступал с задержкой, потому что подслушивающее устройство требовало дополнительного отвода из линии. С телефоном было не все в порядке». Если делать подобные выводы на основании указанных признаков у нас, в России, то очень легко попасть впросак, ибо довольно часто это не соответствует действительности. Как правило, главная причина появления подобного феномена — низкое качество отечественных телефонных каналов связи. Вместе с тем хотя и нельзя принимать категорическое решение о факте прослушивания, ориентируясь «на слух», но при малейшем подозрении будет полезно использование организационных мер защиты, которые, кстати, предложены в вышеупомянутой книге.

**Организационные меры защиты информации в телефонных линиях связи**

Необходимо прежде всего определить порядок ведения деловых бесед по телефону, узаконить круг лиц, допускаемых к тем или иным внутрифирменным секретам, запретить сотрудникам вести служебные переговоры с домашних телефонов. Для передачи особенно важных материалов использовать только устойчивые сети связи (каналы ФАПСИ, МО, «Исток»), а также скремблеры. Если стало известно, что за вами установлен контроль, то можно использовать во время беседы систему условностей и сознательную дезинформацию. Не рекомендуется называть фамилию и отчество собеседника, если это позволяет этикет. Назначая место и время встречи, лучше переходить на условности (типа — пункт № 2 и т. д.), которые должны быть заранее оговорены и органически вписываться в контекст вашего разговора. Эзопов язык должен быть знаком всем сотрудникам фирмы. Правда, как показала практика, система подобного «кодирования» информации не сможет продержаться достаточно долго.

Рекомендуется приучить к определенному порядку ведения телефонных переговоров и членов семьи: они не должны сообщать кому бы то ни было информацию о том, где вы находитесь и когда вернетесь домой. При шантаже со стороны преступных групп не следует звонить со своего телефонного аппарата, чтобы сообщить об этом в службу безопасности, милицию и т. д. Лучше это сделать с телефона-автомата, от соседей и друзей. Надо учитывать, что в маленьких городах телефонные аппараты милиции и органов безопасности могут легко прослушиваться преступными группировками. В этом случае необходимо, чтобы позвонил ваш друг или коллега и, не называя истинной причины, организовал встречу или беседу с представителями данных организаций.

Для защиты телефонных каналов связи необходимо, чтобы распределительная коробка (РК) телефонов фирмы обязательно находилась в помещении офиса и контролировалась службой безопасности или охраной. В случае, если данное требование совершенно невыполнимо, то желательно установить ее в закрывающемся на замок металлическом ящике, оборудованном

сигнализацией. Для ремонта ТА целесообразно приглашать только проверенных специалистов. Желательно заключить договор со специализированной организацией, которая могла бы периодически проводить проверки вашей аппаратуры и линий связи.
Если вы не знакомы с мастером узла связи, собирающимся ремонтировать телефоны в вашем офисе или просто проверить РК, не поленитесь попросить у него служебное удостоверение, позвоните на узел связи и удостоверьтесь, что там действительно работает такой специалист и что именно он получал наряд на работу в вашей фирме. Если данные не подтвердились, срочно принимайте меры. В первую очередь вызовите бригаду для проверки линии и аппаратов. Усильте работу службы безопасности и охраны. Для передачи информации перейдите на запасные каналы связи, в том числе факс, телекс, телеграф (хотя и они, как видно из раздела 1.5, тоже могут контролироваться).
Все перечисленные меры в значительной степени снижают риск потери информации, однако не дают полной гарантии и даже могут привести к целому
ряду дополнительных сложностей в текущей деятельности, если их в дальнейшем не подкрепить техническими мероприятиями.
В крупных организациях имеет смысл создавать собственные службы безопасности (СБ), на которые в числе прочего нужно возложить и-проблемы защиты телефонной связи. Технический отдел СБ в первую очередь должен будет провести следующие основные мероприятия:
>• оценить состояние системы связи (состав, технические характеристики, наличие схем прокладки и т. д.);
**>•** оценить степень конфиденциальности информации, циркулирующей по каналам связи;
**>•** оценить уровень угрозы безопасности со стороны конкурентов, преступников, разведок и т. д.;
>• выявить и оценить степень опасности всех каналов утечки информации через технические средства;
>• организовать взаимодействие с соседними (по зданию) фирмами, правоохранительными органами, учреждениями связи, специализированными организациями по защите информации, имеющими соответствующие лицензии на данный вид деятельности;
>• изучить законодательные и иные документы по защите информации в сетях телефонной связи;
>• провести анализ доступных средств защиты этих сетей; приобрести и установить технические средства защиты информации;
>• провести обучение персонала по применению этой спецтехники;
>• осуществлять постоянный контроль за эффективностью принятых защитных мероприятий;
>• проводить распределение между пользователями необходимых реквизитов защиты (например, паролей или скремблеров) и т. д.
Из этого далеко не полного перечня видно, что организационные меры необходимо дополнить и проведением комплекса технических мероприятий по защите линий телефонной связи.

**Технические методы и средства защиты**

Теперь снова вернемся к проблеме, как все-таки можно достоверно определить факт внедрения в телефонную сеть. Для обнаружения подслушивающих устройств, особенно когда их ставят непрофессионалы, часто достаточно просто провести тщательный внешний осмотр телефонных линий и ТА. Однако даже эта элементарная проверка, как правило, возможна только в пределах зон А и Б (до РК). Контроль в остальных зонах практически неосуществим без привлечения служащих АТС. Впрочем, в связи с тем что подключение «жучков» чаще всего как раз и осуществляется в зонах А и Б, обнаружение подслушивающих устройств или

следов их применения при должном внимании к мелочам более чем вероятно. При проведении осмотра обязательно производится разборка как ТА, так и телефонных розеток. В качестве иллюстрации к этой простой мысли на рис. 2.4.1 показан внешний вид телефонного «жучка» английского производства, вмонтированного в аппарат. Устройство такого рода может быть установлено в считанные минуты и используется в тех случаях, когда нет времени для внедрения более сложных систем. Думаем, не надо быть специалистом по связи, чтобы сообразить, что в телефоне посторонний и совсем небезобидный объект.

В качестве примера практической эффективности этого метода приведем небольшую выдержку из газеты «Коммерсант» (№ 15 от 6 февраля 1999 года): «Сотрудники еженедельника «Самарское обозрение» включили приемник и были поражены, услышав в эфире прямую трансляцию из кабинета своего главного редактора. Сначала журналисты сами пытались найти «жучка», а когда им это не удалось, вызвали милицию. У прибывшего наряда спецтехники не было, но, видимо, оперативники сталкивались с подобными ситуациями. По крайней мере, они в считанные минуты обнаружили два подслушивающих устройства, спрятанных в электрических распределителях. Находки упаковали в полиэтиленовый пакет и отправили на экспертизу. Пока у журналистов есть только одна версия случившегося. Недавно контрольный пакет акций газеты был выставлен на продажу, и им заинтересовалось несколько финансовых структур». Однако, совсем не умаляя действительно высокий профессионализм сотрудников самарского УВД, хотим сказать, что если бы «жучок» ставил тоже «профи», то для его обнаружения потребовалась бы существенно более серьезная проверка.

При проведении такой проверки прозваниваются линии до РК, осуществляется их тестирование на наличие электромагнитных наводок и т. д. Все это достаточно трудоемкий процесс, который уже требует использования специальной аппаратуры контроля линий связи. В ряде случаев необходимо иметь оперативную информацию о текущем со-

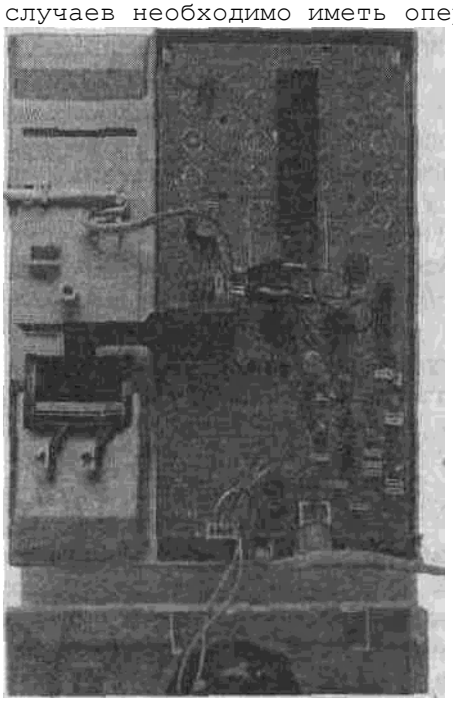


**Рис. 2.4.1. Устройство негласного съема информации, установленное в телефонном аппарате**

стоянии телефонной линии. Главный недостаток большинства приборов этого класса состоит в том, что они только сигнализируют о наличии подслушивающего устройства. Однако есть реальная возможность обеспечить

постоянную безопасность телефонной линии — для этих целей серийно выпускается многочисленная аппаратура защиты различной степени сложности. В свою очередь, каждую из этих двух групп по принципу действия можно разделить на подгруппы.

**Аппаратура контроля линии связи:**

>• анализаторы и индикаторные устройства;
>• кабельные локаторы (последние, в свою очередь, делятся на два типа: рефлектометры и приборы, использующие принципы нелинейной локации);
>• детекторы поля, частотомеры, специальные радиоприемные устройства и универсальные комплексы контроля.

**Аппаратура защиты линий связи:**

>• многофункциональные устройства защиты телефонных линий;
>• устройства уничтожения «закладок»;
>• аппаратура криптозащиты;
>• устройства защиты от пиратских подключений;
>• аппаратура линейного и пространственного зашумления;
>• аппаратура защиты от ВЧ-навязывания.

Детекторы поля, частотомеры, специальные радиоприемные устройства и универсальные комплексы контроля различной степени сложности применяются для обнаружения радиозакладок, установленных в линиях связи. Все эти приборы уже были подробно рассмотрены в главе 2.3, поэтому в данном разделе на них останавливаться не будем. Все отличие в методике поиска телефонного или сетевого «жучка» от поиска обычной радиозакладки будет заключаться в том, что тестовый сигнал подается в проверяемую линию. Остальную аппаратуру рассмотрим более обстоятельно.

### 2.4.2. Аппаратура контроля линий связи

**Индикаторные устройства**

Принцип действия приборов указанного типа основан на измерении и анализе параметров телефонных линий. Основными параметрами, которые наиболее просто поддаются контролю, являются значение постоянной составляющей напряжения в линии и величина постоянного тока, возникающего в линии во время разговора. Кроме того, анализу могут быть подвергнуты изменения активной и реактивной составляющей комплексного сопротивления линии, изменения напряжения в момент снятия телефонной трубки. В более сложных приборах производится анализ и переменной составляющей сигнала. Например, появление в режиме «отбоя» сигнала с частотой более 50 Гц — явный признак того, что к линии подключена аппаратура ВЧ-навязывания или передается модулированный ВЧ-сигнал (т. е. линия используется как канал для «сброса» информации акустической «подслушкой»). На основе проведенных измерений прибор «принимает решение» о наличии несанкционированных подключений или просто сигнализирует об изменении параметров линии. Именно использование достаточно сложного алгоритма принятия решения и отличает анализатор от простого индикатора. Правда, многие специалисты не выделяют последние в отдельный тип, а считают их примитивными анализаторами, настоящее время на рынке спецтехники представлено много моделей анализаторов в ценовом диапазоне от десятков до нескольких тысяч долларов.

Конечно, аппаратура контроля линий связи не обеспечивает полную защиту от злоумышленников, но жизнь им существенно усложняет. Для того чтобы включиться в защищенную линию и не быть обнаруженным, необходимо использовать системы перехвата, которые практически не меняют параметров линии или максимально компенсируют изменения. А это уже подслушивающие приборы совсем другого класса, а значит, и стоимости.

Справедливости ради надо отметить, что анализаторы и индикаторы имеют и целый ряд существенных недостатков.

Во-первых, отсутствуют четкие критерии для установления факта наличия несанкционированного подключения. Телефонные линии (особенно наши)

далеко не идеальны. Даже в спецификации на стандартные параметры сигналов городских АТС предусмотрен большой разброс. Настолько большой, что на разных типах АТС они могут отличаться в несколько раз. Кроме того, параметры меняются в зависимости от времени, загруженности АТС, колебаний напряжения в электросети, влажности и температуры. Сильно влияние и различного вида наводок.

Во-вторых, высока вероятность ложных срабатываний. Более надежны оказываются те приборы, которые просто фиксируют изменение того или иного параметра, предоставляя принимать решение самому пользователю.

В-третьих, самым большим недостатком анализаторов является то, что они могут зафиксировать только небольшую часть устройств перехвата из возможного богатого арсенала злоумышленников. Например, определить факт подключения к реальной линии бесконтактного устройства практически невозможно.

В-четвертых, почти все анализаторы устроены так, что при их установке требуется балансировка под параметры линии. Если при этой операции на линии уже был установлен «жучок», то, естественно, он обнаружен не будет. Мало того, при снятии «подслушки» у анализатора остается «запас», который не позволит выявить факт установки нового устройства съема. И это неудивительно, ведь прибор может реагировать лишь на ухудшение параметров линии. Поэтому линию предварительно надо тщательно проверить.

Однако аппаратура этого типа весьма популярна на рынке спецтехники. Особенно это относится к индикаторам вследствие их очень низкой стоимости. Простейшим индикатором наличия подслушивающих устройств, вполне доступным по цене любому клиенту и работающим достаточно надежно, является устройство типа **ЛСТ-1007**, обычно называемое «Телефонный страж» (рис. 2.4.2). Данное устройство устанавливается на предварительно проверенной телефонной линии (совершенно обязательное условие) и легко настраивается с учетом ее параметров. Питание осуществляется от самой линии. При подключении любых несанкционированных приборов, которые тоже питаются от телефонной сети (например, аппаратура с непосредственным включением в линию, согласно классификации раздела 1.5.1), вырабатывается сигнал тревоги (загорается красная лампочка).

Чтобы был более понятен принцип действия этого несложного прибора, приведем схему простейшего индикатора, который легко сможет сделать радиолюбитель средней квалификации (рис. 2.4.3).

Зарубежным аналогом **ЛСТ-1007** является устройство типа **ST1.** Дополнительно к лампочке на нем установлен стрелочный индикатор (вольтметр),

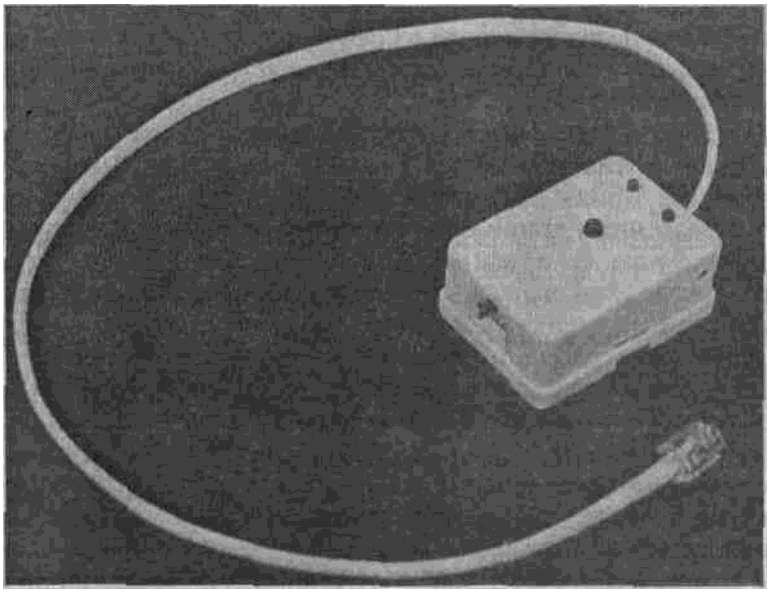


**Рис. 2.4.2. «Телефонный страж», ЛСТ-1007**

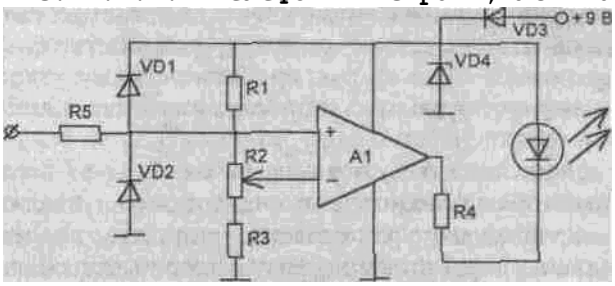



**Рис. 2.4.3. Простейшее индикаторное устройство подключения к телефонной линии**

по степени отклонения стрелки которого в красный сектор шкалы и принимается окончательное решение или о наличии подслушивающих устройств
на линии, или об очередном «броске» параметров сигнала АТС.

**Анализаторы проводных линий и кабельные локаторы**

Телефонный анализатор в простейшем виде представляет собой комбинацию мультимера и прибора, позволяющего обнаруживать переделки в ТА. С помощью мультимера отмечается отклонение от нормального значения ряда параметров (например, напряжения) абонентской линии связи при снятой и положенной телефонной трубке. Повышенное или пониженное по сравнению со стандартным значением напряжение или сопротивление могут означать соответственно параллельное или последовательное подключение подслушивающих устройств. Некоторые типы анализаторов способны инициировать работу и тем самым выявлять подслушивающие устройства, приводимые в действие от сигнала вызова.

Одним из типичных представителей данного класса приборов является портативный анализатор ССТА-1000, выпускаемый фирмой CCS Communication Control. Он позволяет проводить 6 типов контрольных проверок телефонных линий с целью выявления факта подключения подслушивающих устройств, магнитофонов или дополнительных телефонных аппаратов. В ходе этой операции телефонный разъем подключается к гнезду анализатора, а инструкции (последовательность действий) по проведению самой проверки и ее результаты высвечиваются на двухстрочном 80-знако-вом индикаторе, вмонтированном в верхнюю панель прибора. Анализатор осуществляет измерение напряжения, емкости, тока и сопротивления линии в

автоматическом и ручном режимах. В приборе предусмотрена также антенна для выявления подслушивающих устройств с радиопередатчиками (типа «закладок»). Анализатор может быть использован для одновременной проверки 25 телефонных пар. Оформлен он в виде стандартного кейса. Вес — 6,8 кг. Питание — от сети 220 В. Внешний вид прибора приведен на рис. 2.4.4.

Анализатор телефонной линии **SP18-T** обеспечивает обнаружение гальванически подключенных к телефонным линиям устройств несанкционированного съема информации на участке от анализатора до АТС. Он полностью автоматизирован и не требует «чистой линии» на момент подключения. Прибор обеспечивает:

>• контроль нелинейности импеданса (комплексного сопротивления) телефонной линии при разомкнутом и замкнутом шлейфах;

>• определение наличия сигналов ВЧ-навязывания;

>• определение параллельного подключения к линии во время телефонных переговоров.

**Рис. 2.4.4. Анализатор телефонных линий ССТА-1000**

Длительность тестирования — 3—10 мин. Индикация — на ЖКИ-дисплее. Питание — от аккумулятора 9 В или сетевого адаптера. Габариты — 160x160x45 мм. Внешний вид прибора показан на рис. 2.4.5.

У профессионалов в состав комплекта аппаратуры контроля может быть включен **кабельный локатор**. Как было отмечено выше, эти приборы бывают двух видов: рефлектометры и устройства, использующие принцип нелинейной локации.

Рефлектометр, или «кабельный радар», позволяет не только обнаружить факт проникновения, но и определить расстояние до подозрительного места в телефонной линии. Принцип его действия основан на том, что в линию посылается импульс, который должен отразиться от неоднородности сети, возникающей в месте параллельного или последовательного подключения к ней различных дополнительных устройств. Расстояние измеряется с помощью осциллографа, регистрирующего время задержки импульса. Обычно проводятся следующие тесты:

>• тестируется одна двухпроводная линия;

**>•** сравниваются две или более двухпроводные линии;

>• двухпроводная линия с известными параметрами (эталонная) сравнивается с контролируемой.

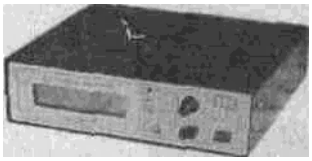


**Рис. 2.4.5. Анализатор телефонных линий SP18-T**

В России существует целая серия подобной аппаратуры — это так называемые испытатели кабельных линий (импульсные) Р5-1А, Р5-5, Р5-8, Р5-9, Р5-10, Р5-11, Р5-13, Р5-13/1, ИКЛ-5. По большому счету, они предназначены для определения по специальным меткам и расчетным формулам расстояния до места повреждения (обрыв, короткое замыкание, пробой между жилами, разбитость пар, асимметрия по постоянному току), но нашли применение и как средство поиска закладных устройств в сетях различного назначения. Характеристика исследуемой линии высвечивается на экране электронно-лучевой трубки.

Рассмотрим в качестве примера некоторые из них.

**Р5-9** — измеритель неоднородности кабеля. В приборе имеется три диапазона измеряемых расстояний: 0... 100; 0... 1000; 0... 10 000 м. Погрешность измерения составляет ±1 % от предельного значения диапазона. Длительность зондирующего импульса выбирается из следующей совокупности значений: 10, 30, 100, 500, 2000 не. Амплитуда зондирующего сигнала изменяется в пределах от 10 до 30 В. Габариты прибора составляют 213x310x455 мм при массе — не более 12,5 кг. Питание возможно как от сети 220 В, так и от встроенного автономного источника (аккумуляторной батареи).

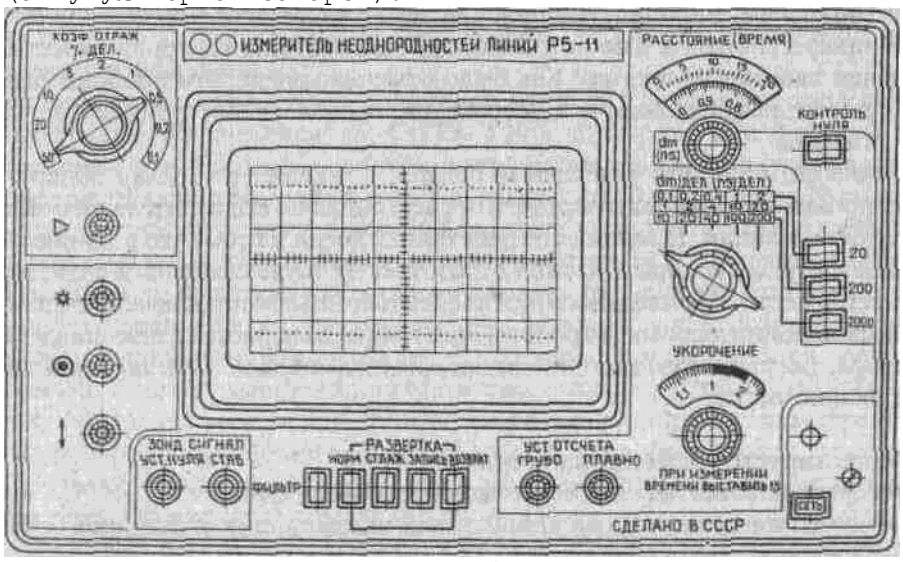



**Рис. 2.4.6. Передняя панель кабельного радара Р5-11**

**Р5-9** может работать на кабелях различных типов с волновым сопротивлением от 10 до 1000 Ом длиной до 10 км при максимальном затухании отраженного сигнала -50 дБ. Разрешающая способность позволяет проводить измерения расстояния до неоднородности на отрезках кабелей длиной всего в 1...1,5 м. По форме, полярности и относительной величине отражения импульсов можно оценить характер неоднородностей и прикинуть их величину (изменение размера сечения, параметров диэлектрического заполнения и т. д.).

**Р5-13** — измеритель неоднородностей телефонных линий. Отличается улучшенными эксплуатационно-техническими характеристиками и большим удобством в работе. Его вес составляет всего 9 кг, а габариты — 120x304x350 мм.

Кроме приборов, основное назначение которых — поиск неисправности при

ремонте линий связи, имеется аппаратура, специально используемая для поиска «жучков». Например, телефонное проверочное устройство ТПУ-5 (рис. 2.4.7), которое предназначено для проверки телефонных линий (кроме спаренных) и позволяет обнаружить как параллельно, так и последовательно подключенные подслушивающие устройства.

В Россию поступает и аналогичная зарубежная аппаратура.

**«Дигифлекс Т12/3»** — импульсный эхометр (Германия). По своим техническим возможностям он существенно не отличается от отечественных аналогов, однако сервисные функции значительно лучше (главное — возможность подключения персонального компьютера, что позволяет производить сравнительные замеры, а также осуществлять распечатку на принтере результатов контроля).

**Основные технические характеристики**

Диапазон измерений ..... 0,5; 1;2,5; 10,20км
Динамический диапазон..... >90 дБ
Память..... 10 рефлексограмм
Длительность импульсов ..... 50; 100; 200; 500; 1000; 2000 нс
Дисплей..... контрастный жидкокристаллический с разрешением 128x256
Габариты .....255x155x250 мм

Системы, производящие анализ телефонной линии на основе принципов нелинейной локации, не получили широкого распространения в связи со сложностью работы и неоднозначностью получаемых результатов. Кроме того, уровень зондирующих сигналов, используемых в этих устройствах, составляет 50...300 В, что недопустимо много для большинства элементов телефонных сетей.

**Рис. 2.4.7. Телефонное проверочное устройство ТПУ-5**

**Рис. 2.4.8. Анализатор проводных линий LBD-50**

Производители утверждают, что дальность обнаружения неоднородностей такими устройствами достигает 5000 м, но на самом деле измеряемое расстояние существенно меньше (реально — до 100 м). Приведем параметры некоторых подобных приборов.

**LBD-50** — анализатор проводных линий. Предназначен для анализа параметров любых проводных линий с целью выявления несанкционированных подключений устройств негласного съема информации (рис. 2.4.8). В основу работы прибора положен метод нелинейной локации.

Прибор позволяет исследовать переходные процессы в линиях и проводить «традиционные» измерения: величины тока, сопротивления утечки и т. п. Он может быть подключен к электросети без отключения напряжения. В

комплект анализатора включено устройство для бесконтактного определения противоположного конца анализируемой линии и поиска ее в жгуте проводов.

**Основные технические характеристики**

Диапазон измерения токов утечки..... 0,1...200 мА
Диапазон измерения сопротивления изоляции .....100кОм...20МОм
Дальность фиксации тестового сигнала в линии ..... до 1 см
Питание от сети переменного тока..... 220 ±20 В, 50 Гц

**«Визир» —** низкочастотный нелинейный детектор проводных коммуникаций. Предназначен для обнаружения средств подслушивания, подключенных к проводным коммуникациям (как силовым, так и слаботочным), с целью съема и передачи информации, а также к цепям питания таких устройств. Внешний вид устройства приведен на рис. 2.4.9.

Принцип действия прибора заключается в подаче в линию зондирующего синусоидального сигнала и регистрации высших гармоник тока, возникающих в полупроводниковых элементах подключенного к линии средства прослушивания. Анализ наличия высших гармоник проводится оператором визуально — путем наблюдения изображения на жидкокристаллическом экране прибора.

**Рис. 2.4.9. Низкочастотный нелинейный детектор «Визир»**

**Основные технические характеристики**

Индикация обнаружения..... визуальная
Мощность постоянного тока в нагрузке блока питания обнаруживаемого средства, не менее..... 1 мВт
Сопротивление подключенной параллельно к обследуемой линии согласующей цепи обнаруживаемого устройства, не более ..... 1 МОм
Сопротивления подключенной последовательно к обследуемой линии согласующей цепи обнаруживаемого устройства, не менее ..... 100 Ом
Длина обследуемых линий, не более ..... 1000м
Напряжение зондирующего сигнала..... 220 В, 50 В
Частота зондирующего сигнала..... 50 Гц
Время задержки подачи зондирующего сигнала в линию..... 20 мс
Напряжение питания..... 220 В, 50 Гц

### 2.4.3. Средства защиты линий связи

**Многофункциональные устройства индивидуальной защиты телефонных линий**

На практике разработаны и широко используются специальные схемы предотвращения прослушивания помещений через ТА, находящиеся в режиме «отбоя». Эти средства могут устанавливаться в разрыв телефонной линии или вставляться в цепи непосредственно ТА. При правильном размещении фильтра удается также нейтрализовать микрофоны, передающие информацию по телефонной линии в длинноволновом диапазоне. Так, на рис. 2.4.10 показана простая, но очень эффективная схема подавления слабых информационных

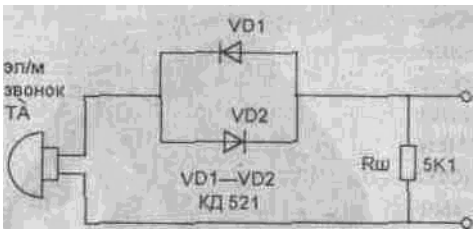



**Рис. 2.4.10. Простейшая схема в линию защиты телефонного аппарата**

сигналов, возникающих в звонковой катушке, при воздействии на нее акустических волн (эффект акусто-электрического преобразования).

Здесь два кремниевых диода, включенных по схеме варистора, образуют зону нечувствительности для малых паразитных токов, которые возникают в обмотке катушки (упрощенная вольт-амперная характеристика диодов приведена на рис. 2.4.11).

В то же время речевой сигнал абонента и напряжение вызова ТА свободно «проходят» через диоды, так как их амплитуда значительно превышает порог нечувствительности этих элементов (0,3...0,5 В). Резистор Rш является дополнительным шунтирующим элементом. Подобная схема, включенная последовательно в звонковую цепь ТА, уменьшает ток в линии, который вызывается наводимой в катушке ЭДС, на 40... 50 дБ.

Наиболее распространенным серийным устройством защиты, работающим по этому принципу, является изделие типа **«Гранит-VIII»**, которое обладает техническими характеристиками, приведенными в табл. 2.4.1.

Кроме **«Гранита-VIII»** значительное распространение получили его аналоги, выпускаемые различными производителями: **«Корунд-М»**, **«Утес-ТА»**, **«Обрыв»**, **«ТА-1»**, **«ТА-2»**, **«ТФ»** и др. Внешний вид некоторых из этих устройств приведен на рис. 2.4.12.

Небольшая доработка выше приведенного устройства позволяет надежно защитить телефон от прослушивания с использованием метода ВЧ-навязывания. Так как объектом ВЧ-воздействия является микрофон ТА (см. подраздел 1.3.5), то достаточно подключить параллельно микрофону конденсатор емкостью 0,01...0,05 мкф (более подробно эти материалы изложены в подразделе 2.4.7). При этом данный конденсатор шунтирует по высокочастотной составляющей микрофонную капсулу, глубина модуляции навязываемого излучения уменьшается более чем в 10 000 раз, что практически делает невозможным извлечение из него информации.


**Рис. 2.4.11. Упрощенная вольт-амперная характеристика встречновключенных полупроводниковых диодов**

**Таблица 2.4.1. Основные характеристики изделия «Гранит-VIII»**

Характеристики /Значения

Затухание в полосе частот 0,15...10 кГц при уровне входного сигнала 10 В, не более /3 дБ

Затухание при входном напряжении 10 В на частоте 50 кГц, не менее /6 дБ

Габариты /95х60х25 мм

Вес /0,2 кг

На рис. 2.4.13 приведен еще один вариант схемы защиты. Ее основное отличие заключается в использовании двух пар кремниевых диодов, шунтирующих конденсаторов и дополнительных катушек индуктивности. Элементы L и С здесь являются дополнительным фильтром ВЧ-сигналов. Эта схема обеспечивает одновременно эффективную защиту от обоих выше перечисленных способов прослушивания.

Кроме рассмотренных простых и дешевых приборов существует целый ряд и достаточно сложных индивидуальных устройств защиты ТА, выполняющих следующие функции:

**>•** изменения напряжения в линии, приводящего к отключению диктофонов с системой автоматического включения при снятии трубки и других устройств, которые используют для работы напряжение телефонной линии;

>• генерации маскирующей речь помехи, которая не мешает разговору, поскольку автоматически фильтруется на всех АТС, зато те, кто подключился на линию до станции, будут слышать только громкое шипение;

>• защиты телефонного аппарата от попыток модификации с целью использования его для прослушивания помещения.

Внешний вид некоторых устройств защиты приведен на рис. 2.4.14. Приведем характеристики наиболее распространенных устройств этого типа.

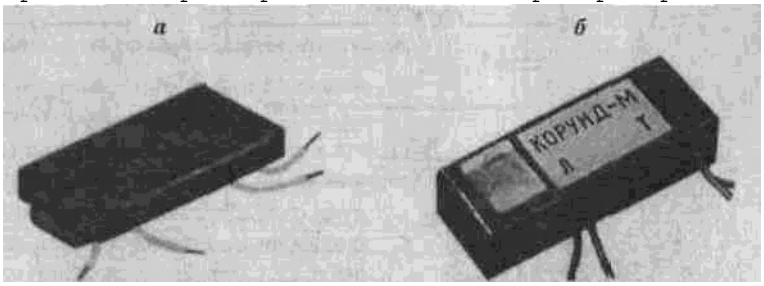



**Рис. 2.4.12. Устройства защиты телефонных аппаратов:**
**а — «Гранит-УЩ»; б — «Корунд-М»**

Phone Guard 2 — устройство индивидуальной защиты. Имеет три основных режима работы.

Режим 1. Самый простой режим, в котором телефонный страж обнаруживает только факт непосредственного подключения к линии подслушивающих устройств с низким сопротивлением, а также параллельное включение постороннего телефона. Как только вы снимете трубку, загорается красный индикатор «PRIV». Пока горит этот индикатор — разговор безопасен. Если произойдет параллельное подключение, индикатор гаснет, а разговор прерывается автоматически.

Режим 2. В данном режиме производится регистрация излучений радиопередатчиков, находящихся в непосредственной близости от ТА, если их работа совпадает по времени с вашим разговором.

Режим 3. Телефонный страж может нейтрализовать некоторые виды подслушивающих устройств (например, телефонные диктофоны с автоматическим включением записи при снятии трубки).

**NG-303** — устройство защиты от утечки информации. Выполняет функции по защите телефонных линий от прослушивания переговоров с использованием различных средств негласного съема информации, а также защите электросетей переменного тока 220 В 50 Гц от несанкционированного их использования для передачи речевой информации (аналогично изделию NG—401).

В отличие от предыдущих аналогичных моделей в этом устройстве реализована возможность сигнализации о «пиратском» подключении к телефонной линии и блокировки несанкционированно подключенного параллельного ТА. Еще одним достоинством является простота настройки изделия.

Фактически это комплекс, состоящий из свипирующего генератора для защиты электросети, а также ряда независимых генераторов для «зашумления» телефонных линий. В нем используются следующие виды излучений:

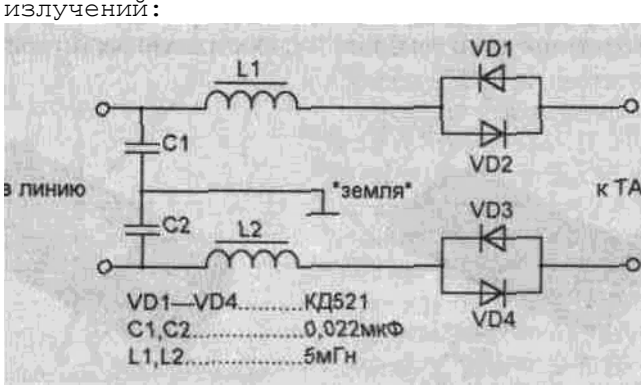



**Рис. 2.4.13. Схема защиты телефонного аппарата от прослушивания за счет эффектов акусто-электрического преобразования и ВЧ-навязывания**

>• синфазная помеха в виде сложного шумоподрбного сигнала с цифровым формированием (М-последовательность) в звуковом диапазоне частот (100 Гц... 10 кГц);

>• парафазная помеха с цифровым формированием (М-последовательность), обеспечивающая подавление радиозакладных устройств в диапазоне частот 30 кГц ...650 МГц.

Устройство обеспечивает эффективное противодействие следующим средствам негласного съема информации:

>• микрофонам, использующим для передачи информации электросеть 220 В;

>• радиопередатчикам, включаемым в телефонную линию как непосредственно (последовательно и параллельно), так и индукционным способом;

>• аппаратуре магнитной записи, подключаемой к телефонной линии с помощью контактных или индукционных датчиков;

>• телефонным аппаратам, факсам, модемам, негласно подключаемым к телефонной линии.

**Основные, технические характеристики**

Гарантированная полоса защиты сигнала..... 80...5000 кГц
Мощность сигнала защиты ..... 5 Вт
Отношение сигнал/шум в устройстве прослушивания телефонного канала, не хуже...-20 дБ
Отношение сигнал/шум в телефонном аппарате, не менее..... 14 дБ
Габариты ..... 205x60x155 мм
Питание..... 220 В

**Shark** — модуль защиты телефонной линии. Предназначен для противодействия несанкционированному съему информации как во время разговора, так и при положенной трубке.

**Основные технические характеристики:**

Регулировка тока в линии в режиме разговора..... 7...30мА
Шумовая помеха в виде псевдослучайной последовательности с ограничением спектра в полосе ..... 8...25кГц
Напряжение шумовой помехи ..... до 25 В
Потребляемая мощность ..... 10Вт
Напряжение питания..... 220В
Включение и регулировка защитных функций.... ручные


**Рис. 2.4.14. Устройства защиты телефонных аппаратов-**
а - N0-303; б - Shark ; в - SI-2001; г - SI-2020; д - Sprut; е - Sprut -MINI;

**Рис. 2.4.14. Устройства защиты телефонных аппаратов (окончание):**
ж — TSU-3000; з — «Барьер-3»; и — «Прокруст-2000»; к — «Прокруст-минипак»; л — «Протон»

**SI-2001** — 4-каналъный прибор защиты телефонных линий. Предназначен для защиты переговоров по телефонным линиям (до четырех одновременно) от утечки информации. Принцип действия основан на маскировке спектра речи широкополосным специальным сигналом. Позволяет защищать переговоры в линии от точки подключения к прибору до АТС и предназначен для эксплуатации как на городских, так и местных (внутренних) линиях.

**Прибор обеспечивает эффективное противодействие:**

- радиопередатчикам, включенным в линию последовательно и параллельно (в том числе с индукционными датчиками и внешним питанием);
- аппаратуре магнитной записи, подключаемой к линии с помощью контактных или индукционных датчиков;
- параллельным ТА и аналогичной аппаратуре;
- аппаратуре ВЧ-навязывания;
- аппаратуре, использующей линию в качестве канала передачи или в качестве источника электропитания.

Прибор обеспечивает защиту линии как при поднятой, так и при положенной трубке ТА.

**Основные технические характеристики**

Количество каналов прибора (количество защищаемых линий)..... 4

Полоса пропускания каналов

№1—№3 ..... 1,5 кГц
№4 ..... 3 кГц
Максимальное значение спецсигнала, генерируемого прибором по линии..... 3 В
Отношение напряжения спецсигнала, генерируемого прибором по линии, к напряжению спецсигнала на клеммах ТА в каналах:
№1—3, не менее..... 50 дБ
Na4, не менее ..... 40 дБ
Переходное затухание между каналами прибора в рабочем диапазоне частот, не менее ..... 100 дБ
Диапазон регулировки тока в линии, не менее ..... 5 мА
Электропитание ..... сеть 220 В
Потребляемая мощность, не более..... 30 Вт
Габариты ..... 170x280x60 мм
Масса, не более ..... 3 кг

**SI-2020** — устройство защиты телефонных линий. Предназначено для защиты переговоров по телефонной линии от утечки информации и обеспечивает:
>• модуляцию тока в телефонной линии широкополосным спецсигналом;
>• цифровую индикацию напряжения в линии;
>• возможность подключения аппаратуры магнитной записи для регистрации переговоров, проводимых по защищенной линии.

Прибор предназначен для эксплуатации в городских линиях с любыми типами АТС и защищает информацию от входа в прибор до АТС.
Он обеспечивает эффективное противодействие следующим средствам съема информации:
>• передатчикам с питанием от линии, включенным в линию последовательно и параллельно;
**>•** аппаратуре магнитной записи, подключаемой к линии с помощью контактных или индукционных датчиков;
>• параллельным ТА и аналогичной аппаратуре;
>• аппаратуре ВЧ-навязывания;
>• аппаратуре, использующей линию в качестве канала передачи или источника питания.

Прибор активизирует при положенной трубке телефонные радиозакладки, что значительно облегчает их поиск; диктофоны, что приводит к холостому прокручиванию ленты; защищает линию как при поднятой, так и при положенной трубке.

**Основные технические характеристики**

Максимальное значение спецсигнала,
генерируемого прибором по линии ..... 40 В
Электропитание ..... сеть 220 В
Потребляемая мощность, не более..... 2 Вт
Габариты ..... 95x135x45 мм
Масса, не более..... 0,3 кг
Время непрерывной работы ..... не ограничено

**Sprut** — электронный модуль. Предназначен для защиты проводных телефонных линий от подключения различных устройств съема информации (параллельных телефонов, трубок, индукционных и емкостных съемников, диктофонов, телефонных активаторов, радиопередатчиков). Кроме того, делает неэффективной работу микрофонов, использующих для передачи информации телефонную линию при положенной трубке. В модуле реализованы следующие защитные функции:
**>•** постоянный контроль телефонной линии на разрыв со звуковой и визуальной индикацией;
>• контроль за напряжением в телефонной линии как при положенной трубке, так и во время разговора;
**>•** постановка заградительной шумовой помехи в случае подключения (в

момент разговора) параллельного аппарата или аналогичной нагрузки;
>• включение состояния «высокий уровень» в момент начала разговора (при этом формируется такой уровень сигнала, что нормальная работа возможна только для защищаемого аппарата);
>• включение регулируемой помехи в телефонную линию во время разговора;
>• постановка помехи в линию при положенной трубке.
Модуль предназначен для работы на телефонных линиях, по своим параметрам соответствующих городским телефонным линиям. Полноценная работа возможна только по схеме: одна телефонная линия — один аппарат.

**Основные технические характеристики**

Помеха ..... Модулированная по амплитуде псевдошумовой последовательностью
Несущая частота ..... 45 кГц
Полоса..... 100...3500 Гц
Повторение последовательности ..... через 24 ч
При положенной трубке несущая..... 12 кГц
Напряжение активной шумовой помехи..... ЗОВ
Порог срабатывания на параллельное
подключение при положенной трубке..... 50В
Порог срабатывания на аварийное падение напряжения в линии..... 5В
Автоматическое включение защитных функций после набора последней цифры номера..... 8 с
Точность измерения напряжения в линии..... 0,5 В
Соотношение сигнал/шум во время разговора... 30 дБ
Потребляемая мощность ..... до 15 Вт
Габариты ..... 60х155х198мм

**SPRUT-MINI** —устройство защиты телефонных переговоров. Предназначено для защиты телефонных разговоров на участке «телефон—АТС» от следующих видов устройств несанкционированного съема информации:
>• бесконтактных индуктивных и емкостных датчиков;
>• радиопередающих устройств, подключаемых параллельно или последовательно;
>• радиопередающих устройств акустического контроля помещения, работающих при опущенной трубке телефона;
>• звукозаписывающих устройств (диктофонов и т. д.), подключаемых к телефонной линии;
>• устройств акустического прослушивания помещения, передающих информацию по телефонной линии («телефонное ухо» и т. п.).
Препятствует нормальной работе параллельного ТА при попытке позвонить с него.
Не требует установки такого же устройства в противоположном ТА, т. е. защищаются телефонные переговоры с любым абонентом.
Служит анализатором состояния телефонной линии и сигнализирует об активизации устройств типа «телефонной ухо», а также о непосредственном подключении подслушивающих устройств.

**Основные технические характеристики**

Питание..... сеть 220 В
Напряжение телефонной линии..... 45...60 В
Потребляемая мощность ..... 2 Вт
Габариты ..... 110х90х50 мм
Масса, не более ..... 500 г

**TSU-3000** — устройство защиты телефонных линий. Предназначено для защиты телефонных линий от различных подслушивающих устройств. Оно блокирует автопуски диктофонов, делает невозможным прослушивание с параллельного телефона, телефонной трубки линейного монтера, подавляет работу телефонных радиозакладок, в том числе с индуктивным съемом информации.

Действие прибора основано на размывании спектра речевого сигнала и уменьшении тока потребления в линии при разговоре, что снижает эффективность последовательно подключенных передатчиков.
Устройство позволяет подключить цифровой вольтметр для контроля изменений, происходящих в телефонной линии, отличается простотой эксплуатации. После включения требуемый режим устанавливается с помощью двух кнопок. Работа устройства контролируется автоматически с использованием светодиодных индикаторов. При разрыве телефонной линии или подключения к линии подслушивающего устройства подается звуковой и световой сигнал тревоги. Изделие позволяет прослушивать телефонную линию на наличие любых звуковых сигналов без снятия телефонной трубки.
Не требует наличия аналогичного прибора у противоположного абонента.
**«БАРЬЕР-3»** — устройство защиты телефонных переговоров. Предназначено для защиты телефонных переговоров на участке от ТА до АТС и обеспечивает:
>• подавление подслушивающих устройств, подключенных к телефонной линии, вне зависимости от их типов и способов подключения (в том числе и с индуктивным способом включения);
**>•** подавление автоматических звукозаписывающих устройств, подключенных к телефонной линии и активизируемых при поднятии трубки;
>• подавление звукозаписывающих устройств с ручным управлением записи;
>• запуск диктофонов, активизируемых голосом, при положенной трубке;
**>•** защиту от ВЧ-навязывания и микрофонного эффекта, позволяющих прослушивать акустику в помещении через ТА с положенной трубкой;
>• блокирование работы микрофонов, работающих по телефонной линии;
>• блокирование работы подключенного к телефонной линии параллельного ТА;
**>•** цифровую индикацию напряжения телефонной линии и напряжения отсечки;
>• возможность подключения к телефонной линии звукозаписывающей аппаратуры для архивации телефонных переговоров.

**Основные технические характеристики**

Защищаемый участок телефонной линии ..... от ТА до АТС
Уровень маскирующего шума..... до 40 В
Напряжение отсечки ..... до 50 В
Потребляемая мощность, не более..... 5 Вт
Напряжение питания..... 220 В, 50 Гц
Габариты ..... 220x110x50 мм
Комплект поставки: основной блок «Барьер-3»; сетевой шнур питания; телефонный шнур «евростандарт»; телефонный шнур с вилкой; телефонный шнур с розеткой; шнур соединительный к диктофону; пульт дистанционного управления (ДУ); кнопка ДУ.

**«Прокруст ПТЗ-003»** — прибор защиты телефонной линии. Предназначен для защиты телефонных переговоров от прослушивания на участке от ТА до городской АТС. Защита осуществляется путем изменения параметров стандартных сигналов.
Изделие имеет цифровой дисплей — указатель напряжения на телефонной линии и световой индикатор снятия телефонной трубки. В нем предусмотрено три режима подавления («Уровень», «Шум», «ВЧ-помеха»), которые могут включаться независимо друг от друга, имеется возможность экстренного отключения всех режимов защиты, подключения диктофона для записи телефонных переговоров.
Режим «Уровень» позволяет поднимать напряжения в телефонной линии во время разговора. В режиме «Шум» в линию подается шумовой сигнал звукового диапазона частот при положенной на рычаг телефонной трубке. В режиме «ВЧ-помеха» в линию подается высокочастотный помеховый сигнал вне зависимости от положения телефонной трубки.

**Основные технические характеристики**

Максимальное поднятие постоянного
напряжения на линии в режиме «Уровень» ......до 35 В
Амплитуда «белого» шума в режиме «Шум» .......до 10 В
Диапазон шумового сигнала в режиме «Шум» ..... 50 Гц... 10 кГц
Максимальная амплитуда помехи в режиме
«ВЧ-помеха» ..... до 35 В
Напряжение на диктофонном выходе ..... 10 мВ
Питание .....220 В, 50 Гц
Потребляемая мощность, не более..... 10 Вт

**«Прокруст-2000»** — телефонный модуль для комплексной защиты телефонной линии от прослушивания. Позволяет осуществлять обнаружение подключенных телефонных «закладок» и подавлять их путем постановки активных помех. Предусмотрена защита помещений от прослушивания с использованием методов ВЧ-навязывания.

Прибор обеспечивает ложное срабатывание звукозаписывающей аппаратуры, снабженной системой VOX и подключенной в телефонную линию в любом месте от модуля до АТС (это приводит к непродуктивному расходу пленки и батарей питания звукозаписывающей аппаратуры).

Защитный модуль легко интегрируется в конфигурацию сети офисной мини-АТС. Предусмотрено временное отключение защиты для предотвращения сбоев при наборе номера.

**Основные технические характеристики**

Напряжение питания ..... 220 В, 50 Гц
Максимальная потребляемая мощность ..... до 10 Вт
Габариты .....47x172x280 мм

**«ПРОКРУСТ-минипак»** — прибор защиты телефонной линии. Предназначен для защиты городской телефонной линии от ТА до АТС. Он позволяет.

>• подавлять работу различных типов телефонных радиозакладок, в том числе с автономным питанием и индуктивным способом подключения к линии (путем постановки активных помех);
>• защищать ТА от ВЧ-навязывания;
**>•** автоматически блокировать попытки прослушивания телефонного разговора с параллельного аппарата;
**>•** подавлять нормальную работу звукозаписывающих устройств, подключенных к линии с помощью контактных или бесконтактных адаптеров;
>• превентивно воздействовать на звукозаписывающую аппаратуру, оборудованную системой VOX с целью холостого сматывания пленки и вырабатывания заряда батарей питания.

**Основные технические характеристики:**

Напряжение питания..... 220 В, 50 Гц
Максимальная потребляемая мощность..... до 10 Вт
Габариты ..... 62x155x195мм

**«ПРОТОН»** —устройство комплексной защиты телефонной линии. Оно обладает следующими возможностями:

>• визуальной и звуковой (отключаемой) индикацией о нарушении целостности телефонной линии (короткое замыкание, обрыв);
>• цифровой индикацией постоянной составляющей напряжения в телефонной линии во всех режимах работы;
**>•** развязкой ТА от телефонной линии при положенной трубке (питание осуществляется от отдельного стабилизированного внутреннего источника тока, что исключает использование резонирующих свойств электромагнитных вызывных устройств);
>• постановкой шумовой помехи в звуковом диапазоне частот (отключаемой) в телефонную линию при положенной трубке (обеспечивает активизацию диктофонов, препятствует прослушиванию помещения);
>• автоматическим включением режима минимального тока в телефонной линии без ухудшения качества связи после набора номера абонента;

>• обнаружением и противодействием попытке непосредственного прослушивания телефонной линии во время разговора (с параллельного аппарата, низкоомных наушников и др.).

Помимо перечисленных сложных универсальных устройств защиты существует целый ряд технических средств, предназначенных исключительно для линейного зашумления телефонных каналов передачи информации. О них подробно будет рассказано в п. 2.4.6.

Приборы указанных типов позволяют защитить телефонную линию практически от всех видов подслушивающих устройств. Достигается это путем подмешивания в линию различного рода заградительных сигналов и изменения стандартных параметров телефонной линии (обычно в разумных пределах изменяется постоянная составляющая напряжения и ток) во всех режимах работы. Для того чтобы помеха на линии не очень сильно мешала разговору, она компенсируется перед подачей на ТА владельца прибора. Чтобы помеха не мешала второму абоненту, она подбирается из сигналов, которые сильно затухают в процессе прохождения по кабелю и легко фильтруются абонентским комплексом городской АТС. Чтобы помеха хорошо воздействовала на аппаратуру перехвата, ее уровень должен быть в несколько раз выше уровня речевого сигнала в линии.

Указанные помехи воздействуют на входные каскады и блоки питания аппаратуры негласного съема информации. Воздействие приводит к перегрузке входных цепей и выводу их из линейного режима. Как следствие злоумышленник слышит только шумы в своих наушниках. Изменение режима линии приводит к «обману» систем принятия решения, встроенных в некоторые виды подслушивающих устройств. В результате начинается бесполезное расходование ограниченных ресурсов, например звукового носителя или элемента питания. Если в нормальных условиях некий передатчик работал периодически (только во время ведения телефонного разговора), а, как известно, автоматическая система регистрации включается только при наличии радиосигнала, то теперь она будет работать постоянно, запас пленки быстро кончится и злоумышленнику придется использовать оператора, что очень часто может быть неприемлемо. Все вышесказанное свидетельствует о достаточно высокой эффективности этого способа защиты, однако ему присущи и некоторые недостатки.

Во-первых, обеспечивается защита линии только на участке от самого прибора до городской АТС. Поэтому остается опасность перехвата информации со стороны противоположного абонента.

Во-вторых, поскольку частотный спектр помехи располагается выше частотного спектра закрываемого сигнала, то теоретически достаточно легко очистить сигнал от помехи. Правда, такая аппаратура, имеющая достаточно большие габариты и высокую стоимость, применяется только стационарно, поэтому, как правило, состоит в арсенале спецслужб и практически недоступно большинству потенциальных злоумышленников.

В-третьих, даже при наличии двух комплектов не обеспечивается защита от аппаратуры прослушивания, устанавливаемой на городской АТС.

Зная о принципиальных недостатках, разработчики стараются компенсировать их обеспечением комплексного подхода к решению задач защиты телефонных линий. Для этого в состав прибора вводятся системы для обнаружения несанкционированных подключений; порой такие системы ничем не уступают лучшим анализаторам телефонных линий, причем пользователь получает это в дополнение к основным защитным функциям. Наиболее «навороченные» приборы позволяют вести борьбу и с малогабаритной техникой перехвата речевой информации из помещений в промежутках между переговорами. Привлекательной стороной является наличие многих сервисных функций.

**Устройства уничтожения закладок**

Для практического решения задач защиты информации нашли применение устройства, получившие у специалистов название «телефонные киллеры». Принцип их действия основан на подаче высоковольтного напряжения в телефонную линию. В результате уничтожаются все подключенные малогабаритные устройства. Средство действительно радикальное, но беда в том, что использование данной техники даже с минимальными отступлениями от инструкции по эксплуатации может привести к выводу из строя параллельно подключенных ТА, факсов, модемов, а так же оборудования мини- и городской АТС. Приведем характеристики некоторых подобных устройств.

**Bugroaster**—электронный модуль для уничтожения закладных устройств. Предназначен для физического уничтожения устройств несанкционированного съема информации, гальванически подключенных к телефонной линии. Генерирует серию коротких ВЧ-импульсов, приводящих к разрушению микросхем устройств, подключенных к телефонной линии. Прибор предназначен для зачистки линии в ближней зоне (на расстоянии не менее 200 метров), но обычно только до РК. Применяется в двух основных режимах работы:

>• линия отсоединена от АТС (в коммутационной коробке), провода разомкнуты;

>• линия отсоединена от АТС, провода замкнуты накоротко.

Это позволяет уничтожать закладные устройства, подключенные к линии как последовательно, так и параллельно. Основные отличия от аналогов:

**>•** возможность работы в ручной и автоматическом режимах;

>• современный дизайн;

>• наличие панели, отображающей информацию о работе прибора;

**>•** специально сформированный электрический импульс, позволяющий более эффективно уничтожать устройства несанкционированного съема информации.

**Основные технические характеристики**

Напряжение импульса..... 1500В
Длительность импульса ..... 400 мс
Время непрерывной работы в автоматическом режиме ..... 10 мин
Напряжение питания..... 220 В, 50 Гц
Габариты ..... 60x155x198 мм

**«Кобра»** — выжигатель телефонных закладных устройств. Предназначен для предотвращения прослушивания абонентских телефонных линий с помощью устройств несанкционированного доступа, установленных в телефонные линии с непосредственным параллельным или последовательным подключением. Принцип работы — электрическое уничтожение (прожигание). Внешний вид прибора приведен на рис. 2.4.15.

**Рис. 2.4.15. Выжигатель телефонных закладок «Кобра»**

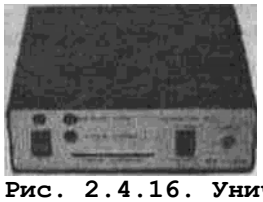


**Рис. 2.4.16. Уничтожитель телефонных передатчиков ПТЛ-1500**

**Основные технические характеристики**

Напряжение на выходе, не менее..... 1600В
Время непрерывной работы в ручном режиме ..... 10 мин

Время непрерывной работы в автоматическом режиме..... 20с
Питание ..... 220 В, 50 Гц
Габариты ..... 65х170х185 мм

**КС-1300** — генератор импульсов. Предназначен для уничтожения подслушивающих устройств, установленных в телефонную линию.

**Основные технические характеристики**

Количество подключаемых телефонных
линий..... 2
Временные интервалы, устанавливаемые
таймером..... от 10 мин до 2 суток
Мощность «прожигающего» импульса..... 15 Вт
Время непрерывной работы в автоматическом режиме..... 24 ч
Питание ..... 220 В, 50 Гц
Габариты ..... 170х180х70 мм

**ПТЛ-1500 —** уничтожитель телефонных передатчиков. Предназначен для вывода из строя радиопередающих устройств негласного съема информации, подключенных к абонентской телефонной линии параллельным или последовательным способом. Принцип действия основан на подаче в линию высоковольтных импульсов, воздействующих на входные каскады подключенных устройств. Изделие имеет функцию блокировки при неправильном подключении к линии. Внешний вид прибора приведен на рис. 2.4.16.

**Основные технические характеристики**

Напряжение на выходе, не менее..... 1500 В
Напряжение питания..... 220 В, 50 Гц
Время непрерывной работы..... 10 мин
Габариты ..... 65х170х185 мм

### 2.4.4. Криптографические методы и средства защиты

Радикальной мерой предотвращения подслушивания телефонных разговоров является использование криптографических методов защиты. Проблемы защиты информации волновали человечество с незапамятных времен. Так, первые системы шифров ученые встречают в Древнем Египте и Древней Греции, Риме и Спарте, используемые задолго до Рождества Христова. Заботились о секретности информация и правители Венеции еще в XVI веке. Без знания специального ключа нельзя прочитать труды многих ученых средневековья — одни боялись преследования инквизиции, другие заботились о пальме первенства, третьи хотели, чтобы их знания достались только ученикам. Примеры достаточно сложных зашифрованных текстов археологи встречают и в русских берестяных грамотах XII—XIII веков. Первые технические системы начали разрабатываться сразу после изобретения телефона. Так, в США в 1875 году была подана заявка на изобретение, относящееся к закрытию телефонной связи. Да и по сегодняшний день в госструктурах самой распространенной мерой защиты каналов связи остается использование криптографических методов закрытия информации.

В настоящее время для защиты телефонных сообщений применяют два принципиально различных метода — **аналоговое** преобразование параметров речи и **цифровое** шифрование. Рассмотрим оба способа защиты.

**Аналоговое преобразование**

При аналоговом скремблировании изменяются характеристики исходного речевого сигнала таким образом, что результирующий сигнал становится неразборчивым, но занимает ту же полосу частот. Это дает возможность без проблем передавать его по тем же каналам связи, что и обычную речь. При использовании этого способа закрытия сообщений речевой сигнал может подвергаться следующим преобразованиям:

**>•** частотной перестановке;
>• временной перестановке.

В значительном количестве приборов кодирования до сих пор применяется инверсия частотного спектра (одни из видов частной перестановки). Известно, что при гетеродинном способе преобразования сигнала на выходе преобразова-

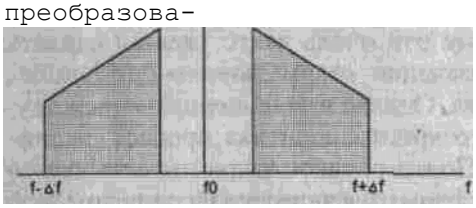



**Рис. 2.4.17. Спектр амплитудио-модулированного сигнала**

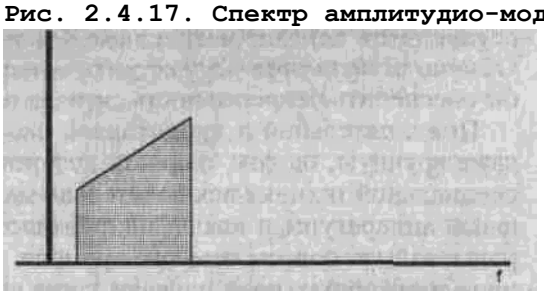



**Рис. 2.4.18. Однополосный сигнал с инвертированным спектром**

теля амплитудно-модулированный сигнал имеет частотный спектр, представленный на рис. 2.4.17.

Вся информация сосредоточена в боковых составляющих слева и справа от несущей частоты. В передающем устройстве одна из полос подавляется фильтром, а другая усиливается, инвертируется (спектральные составляющие на оси частот меняются местами) и подается в канал связи (рис. 2.4.18).

Случайно подключившийся к линии человек не сможет ничего разобрать в таком сигнале, кроме невнятного бормотания. Однако корреспондент, которому адресовано это сообщение, примет его нормально, так как его приемник вновь преобразует сигнал с инвертированным спектром в первоначальный вид.

В более сложных системах речь дробится на определенные, равные по длительности временные участки (интервалы коммутации) продолжительностью от 0,2 до 0,6 с. В пределах этого участка происходит дополнительное дробление на более мелкие участки длительностью 30...60 мс. Всего таких маленьких участков речи может быть от нескольких единиц до нескольких десятков. Эти информационные интервалы до передачи в линию связи записываются в каком-либо запоминающем устройстве, «перемешиваются» между собой по определенному закону, после чего сформированный таким образом сигнал передается в линию связи. На приемном конце линии связи, где алгоритм перемешивания известен, осуществляется обратный процесс «сборки» исходного сигнала (рис. 2.4.19).

К преимуществам этого вида закрытия относится относительная простота технической реализации устройства, а следовательно, низкая стоимость и малые габариты, возможность передачи зашифрованного речевого сигнала по стандартному телефонному каналу и хорошее качество восстанавливаемого исходного сообщения. Главным недостатком метода является его относительно низкая стойкость к несанкционированному восстановлению. Вследствие того что сигнал является непрерывным, у дешифровщика после записи и выделения участков (а это довольно легко сделать, так как в состав сигнала приходится вводить метки, определяющие начало участков) появляется возможность осуществить декодирование даже без знания примененной системы ключей. Обычно попытаются осуществить «стыковку» участков таким образом, чтобы обеспечить непрерывность сигнала на

стыках.
При тщательной и кропотливой работе это очень часто удается сделать даже вручную, однако скорость восстановления «нормального» сигнала без специальной техники исключительно мала. Однако при наличии соответствующей аппаратуры и квалифицированного криптоаналитика процесс дешифровки займет совсем немного времени. Поэтому такое закрытие есть смысл применять только в тех случаях, когда информация является не слишком ценной или когда ее значимость теряет свою актуальность через совсем небольшой промежуток времени.
Несколько более стойкий код получается тогда, когда тот же принцип дробления и перемешивания применяется в отношении частоты. В этом случае с помощью системы фильтров вся полоса частот стандартного телефонного сигнала делится на некоторое количество частотных полос, которые перемешиваются в заданном порядке. Как правило, такое перемешивание осуществляется по псевдослучайному закону, реализуемому генератором ключа. Перемешивание частотных полос осуществляется со скоростью 2...16 циклов в секунду, т. е. одна комбинация длится 60... 500 мс, после чего она заменяется следующей. В свою очередь спектры этих сигналов могут находиться как в прямом, так и в инверсном виде. В ходе разговора кодовые комбинации могут меняться с некоторой цикличностью, однако при этом должна осуществляться очень жесткая синхронизация преемника и передатчика. Принцип частотных перестановок показан на рис. 2.4.20.
Наиболее высокий уровень стойкости при аналоговом кодировании получается с помощью объединения обоих способов. При этом они хорошо дополняют друг друга: временные перестановки разрушают смысловой строй сообщения, а частотные преобразования перемешивают гласные звуки. Количество частотных полос обычно берется не больше 5...6.
Так, временной способ обработки используется в аппаратуре криптозащиты **TRS 769** (компания Thomson—CSF). В этом устройстве производится запись речевого сигнала в память с последующим образованием выборок из 24-мс сегментов, которые, в свою очередь, рассеиваются в псевдослучайной последовательности с образованием 14 групп. Далее сигнал объединяется с обратным псевдослучайно распределенным спектром, что еще больше защищает исходное сообщение. Амплитуды сегментов речевых сигналов поддерживаются на уровне ниже среднего уровня обычных звуков речи. Применение такого метода позволяет создать полную неопределенность относительно положения по времени каждого сегмента, повышая тем самым уровень защиты системы. Более того, сам закон, управляющий временной обработкой речевого сигнала, меняется от сегмента к сегменту неповторяющимся и непредсказуемым способом, поскольку он тоже контролируется сигналами псевдослучайной последовательности.

**Рис. 2.4.19. Кодирование методом перемешивания**

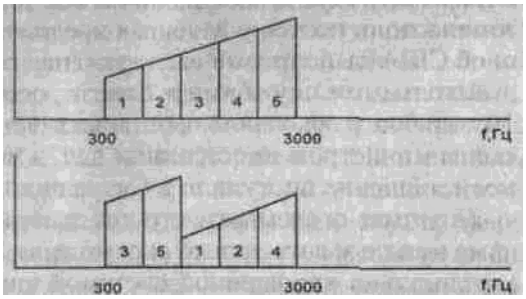



**Рис. 2.4.20. Кодирование методом частотных перестановок**

Таким образом, если необходимо получить действительно надежную защиту, то при выборе аналогового скремблера следует обращать внимание не столько на количество возможных ключевых комбинаций («изюминка» любой рекламы), сколько на сложность преобразований, которые в нем применены.

В самых простейших скремблерах, защищающих лишь от прямого прослушивания дилетантами, используются только частотные перестановки и инверсии, при этом количество каналов не превышает 4, а интервалы коммутации — постоянная величина.

В скремблерах среднего класса, обеспечивающих гарантированную стойкость на время до нескольких часов, уже применяются частотно-временные перестановки с числом частотных каналов от 5 до 10.

В сложных скремблерах, обеспечивающих гарантированную стойкость до нескольких дней, должны быть переменными интервалы коммутации, использоваться частотно-временные перестановки с большим (более 10) количеством частотных каналов и переставляемыми временными интервалами. Количество возможных ключевых комбинаций, как минимум, должно быть более $10^{15}$.

Следует обращать внимание и на то, какой вид связи поддерживает скремблер:

>• симплексный (передача информации только в одном направлении);

>• полудуплексный (поочередный обмен информацией между двумя абонентами);

>• дуплексный (одновременный двусторонний обмен).

Данное обстоятельство в сочетании с «человеческим фактором» иногда оказывает существенное влияние на защиту информации. В качестве примера можно привести следующий интересный факт, взятый из книги, с цитаты из которой мы начали этот раздел.

«Мубарак (президент Египта) недолюбливал закрытую систему телефонной связи, поставленную Соединенными Штатами. Она представляла собой аппарат с ручным переключением на «разговор» и «прослушивание» (полудуплексный скремблер). При пользовании им вести одновременный обмен мыслями было невозможно, поэтому Мубарак предпочитал обычный телефон. Администрацией США было отдано распоряжение об усилении сбора информации разведывательными службами в Египте, особенно АНБ при помощи спутников. 10 октября рано утром был перехвачен телефонный разговор Мубарака со своим министром иностранных дел, и через полчаса это совершенно секретное сообщение поступило в Ситуационную комнату Белого дома».

Практика показывает, что для деловых бесед, а не отдачи команд необходимо использовать только скремблеры, работающие в дуплексном режиме с максимально упрощенной системой управления (в наилучшем случае переключение должно осуществляться нажатием одной кнопки).

Примером неплохого скремблера, реализующего вышеописанные алгоритмы, может служить устройство компании Thomson-CSF.

**TRS 769** — аналоговый скремблер. Производит запись речевого сигнала в электронную память с последующим образованием выборок из 24-мс

сегментов, которые, в свою очередь, рассеиваются с помощью специально генерируемой псевдослучайной последовательности с образованием 14 групп. Далее сигнал объединяется с обратным псевдослучайно распределенным спектром, что еще больше защищает исходное сообщение. Амплитуды сегментов речевых сигналов поддерживаются в позиции ниже среднего уровня обычных звуков речи. Применение такого метода позволяет создать полную неопределенность относительно положения по времени каждого сегмента, повышая тем самым уровень защиты системы. Более того, сам закон, управляющий временной обработкой речевого сигнала, меняется от сегмента к сегменту неповторяющимся и непредсказуемым способом, поскольку он тоже контролируется сигналами псевдослучайной последовательности.

Теперь рассмотрим цифровой способ закрытия, при котором речевой непрерывный сигнал предварительно преобразуется в дискретный вид. Согласно одной из основных теорем теории информации любой непрерывный сигнал может быть без потерь заменен последовательным набором своих мгновенных значений, если они берутся с частотой, не менее чем в 2 раза превышающей самую высокочастотную составляющую этого сигнала. Для стандартного телефонного канала это означает, что такая дискретизация должна происходить с частотой не менее 6 кГц, так как верхняя частотная составляющая телефонного сигнала ограничивается верхним частотным пределом телефонного канала, равным всего 3 кГц.

Максимальное расстояние между точками t1, t2, t3,... на временной оси не должно превышать T=1/2F, где F — максимальная частотная составляющая непрерывного сигнала (рис. 2.4.21). В этом случае непрерывная кривая полностью описывается последовательностью значений [Ai] и временным интер-

**Рис. 2.4.21. Пример временной дискретизации непрерывного сигнала**


валом At. Если мы представим эти значения в виде набора чисел, то переведем сигнал в цифровую форму. Теперь эти числа можно будет легко зашифровать любым известным способом. В этом плане способ цифрового шифрования является более универсальным, и на рынке предлагаются такие типы скремблеров, которые могут шифровать все виды передаваемой информации: от буквенно-цифровой до изображений. При этом все виды сигналов предварительно преобразуются в цифровую форму. В канал связи выдается набор дискретных знаков (как правило, нулей и единиц).

Однако при реализации этого способа кодирования возникают и некоторые особенности.

**Первая особенность** — это необходимость обеспечить довольно быструю выработку огромного объема символов шифра, естественно, если мы хотим сохранить высокое качество сигнала. Если надо передать минимально необходимые 6000 мгновенных значений сигнала в секунду, а его динамический диапазон равен, скажем, 20 дБ (это означает, что максимальная амплитуда сигнала в 10 раз больше его минимального значения), то в 1 с нужно сформировать не менее 6000•4=24 000 двоичных знаков шифра (дело в том, что для представления числа 10 в двоичной системе счисления требуется 4 двоичных знака), т. е. скорость формирования шифра и передачи кодированной информации в линию в этом случае должна быть не менее 24 кбит/с, что достаточно проблематично осуществить при использовании стандартного телефонного канала.

Следовательно, **второй особенностью** при цифровом шифровании речевого

сигнала является требование о наличии гораздо более широкой полосы частот для передачи сигнала в зашифрованном виде, чем имеется у стандартного телефонного канала. Это сильнейшее ограничение на применение метода цифрового шифрования, работающего по такой схеме. Только использование специфичных характеристик речевого сигнала и применение различных сложных технических и математических алгоритмов позволяет резко сузить требуемую полосу и передать зашифрованный цифровым способом речевой сигнал по стандартному телефонному каналу.
Обычно для преобразования речевого сигнала используется так называемый вокодер — устройство, выделяющее существенные параметры речи и преобразующее их в цифровую форму. Однако в этом случае, хотя речь и сохраняет требуемую смысловую разборчивость, опознать собеседника по тембру голоса часто бывает затруднительно, так как голос синтезируется речевым синтезатором и имеет однообразный «металлический» оттенок. Правда.
если для сигнала, зашифрованного цифровым способом, использовать канал с широкой полосой (ВОЛС или радиорелейную связь), то можно сделать качество речевого сигнала достаточно высоким.
Практика показала, что для обеспечения более-менее нормальной работы телефона с устройством защиты, при использовании стандартных отечественных телефонных каналов, скорость передачи информации на выходе блока шифрации, а значит и вокодера, не должна превышать 4800 бит/с. При этом слоговая разборчивость достигает 99 % при вполне удовлетворительной узнаваемости голоса абонента. Кстати, обычный телефонный канал считается каналом среднего качества, если обеспечивает слоговую разборчивость порядка 85... 88 %.
По результатам ряда исследований на московских телефонных линиях получены следующие данные: нормальную работу на скорости передачи 2400 бит/с обеспечивают почти 90 % каналов связи, на скорости 4800 бит/с — уже только 60 % и на скорости 9600 бит/с — всего 35 %. Следовательно, наиболее надежную работу обеспечит аппаратура со скоростью передачи информации 2400 бит/с. В идеале слоговая разборчивость должна быть не хуже, чем в обычном телефонном канале.
При цифровом шифровании речевого сигнала сложной проблемой (вследствие высоких скоростей передачи информации) является и проблема ввода ключей, а также проблема синхронизации. Необходимо добиться того, чтобы шифраторы на приемном и передающем концах линии связи начинали работать строго одновременно и не уходили ни на один такт во время всего сеанса. При этом должно сохраниться такое ценное качество телефонной связи, как удобство ведения разговора и быстрота вхождения в связь. Это удается достичь только за счет существенного усложнения аппаратуры, зачастую с введением в ее состав комплексов компьютерного типа. Поэтому пусть покупателя не удивляет очень высокая стоимость хорошего цифрового скремблера: поверьте, это совсем не прихоть продавца. Зато к несомненным достоинствам систем с цифровым шифрованием можно отнести высокую надежность закрытия информации, особенно при использовании стандартизированных на государственном уровне алгоритмов шифрования, таких, как DES (США) и ГОСТ 28147—89 (Россия).
Другим преимуществом этих систем является возможность применения открытого распределения ключей: в такой аппаратуре перед каждым сеансом связи передатчик и приемник автоматически обмениваются открытыми ключами, на основе которых вычисляется секретный сеансовый ключ. Использование этого метода снимает проблему изготовления и рассылки ключей, а также исключает утечку информации из-за недобросовестного хранения и обращения с ключевыми носителями. Недостатками устройств этого класса помимо высокой стоимости является техническая сложность, неустойчивая работа в каналах с большим затуханием и низкая

узнаваемость голоса абонента.
Сравнительная характеристика двух принципов закрытия речевого сигнала (аналогового и цифрового) приведена в табл. 2.4.2.

**Таблица 2.4.2. Сравнительная характеристика аналогового и цифрового принципов закрытия речевого сигнала**

Наличие переговоров в линии связи /Есть отчетливые признаки /Нет никаких признаков, т.к. при отсутствии переговоров в линию идет чистый шифр

Распределение амплитуды сигнала /Есть ритм и громкость. /Однородная двоичная последовательность

Остаточная разборчивость /Есть признаки начала слова и фразы, паузы /Постоянный однородный шум

Кратковременный спектр сигнала /Спектральные характеристики неоднородны /Однородный

При ведении переговоров работа генератора псевдослучайной последовательности происходит по заданному алгоритму, причем начальная установка для каждого нового разговора вырабатывается и устанавливается в шифраторе заново сразу после ввода ключа. В по-настоящему хорошем скремблере синхронизация осуществляется настолько быстро, что собеседники этого просто не замечают. Выпускаются также универсальные телефонные шифраторы, которые могут работать с различными видами линий связи. При этом степень закрытия остается одинаково высокой, а качество речи тем выше, чем шире полоса пропускания канала. Такая универсальность достигается с помощью модемов и дополнительных связных устройств (рис. 2.4.22).
Преимущества цифрового метода шифрования над аналоговым хорошо видны из таблицы. Однако они достигаются за счет отказа в большей части случаев от стандартного телефонного канала или за счет применения сложной и очень дорогостоящей аппаратуры. Ясно, что когда интенсивность переговоров невысока, применение таких устройств может стать экономически неоправданным. Основной характеристикой цифровых шифраторов является применение того или иного криптографического алгоритма. При этом надежность алгоритма считается высокой, если количество ключевых комбинаций более $10^{25}$. Следует помнить, что длина ключа у таких устройств порядка 30 цифр, это крайне затрудняет его ввод с клавиатуры. Следовательно, при приобретении такого оборудования необходимо обращать внимание на то, в какой форме выполнен ключевой носитель, насколько он надежен и прост в обращении. Если же, например, куплен более дешевый прибор с ручным вводом ключа, то при необходимости срочно позвонить не надо давать волю эмоциям, набирая номер вместе с длиннющим ключом, — «нервные клетки не восстанавливаются».
Государственные органы всех стран также существенное внимание уделяют защите телефонных переговоров. Так, главным направлением деятельности

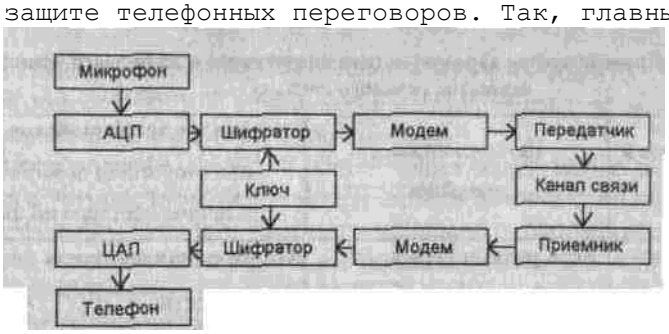



**Рис. 2.4.22. Схема организации закрытого канала связи**

по защите линий связи АНБ считает установку во всех правительственных

учреждениях и на фирмах подрядчиках Пентагона специальных защищенных ТА по программе **STU** (Secure Telefon Unit). В настоящее время наиболее распространены изделия третьего поколения типа STU-3, причем в некоторых компаниях установлено более ста комплектов. Всего в США используется более 700 тысяч телефонов данного типа (цена в США порядка 2000 $).

Телефон **STU-3** внешне похож на обычный ТА, но он дает возможность вести телефонные переговоры в открытом режиме и обмениваться цифровой информацией со скоростью 2400 бит/с в защищенном режиме.

Ключи для сотрудников правительственных учреждений изготовляются в АНБ, а для фирм-подрядчиков — корпорацией GTE.

Для включения аппарата в защищенный режим пользователь вставляет ключ (в виде пластиковой карточки) в приемное устройство телефона. В память ключа занесены следующие идентификационные данные:

>• фамилия и имя пользователя;

>• название фирмы;

>• высший гриф секретности информации, к которой он допущен.

Когда связь установлена, идентификационные данные пользователя и категория его допуска высвечиваются на дисплее аппарата его собеседника. Аппаратура рассчитана на 4 уровня секретности. Переход в закрытый режим может осуществляться как до начала, так и в процессе разговора.

После того как оба абонента вставили свои ключи в аппарат и нажали кнопку «защита», идентификационные данные каждого ключа направляются в компьютер АНБ, где проверяется, не происходила ли утрата одного из ключей.

В настоящее время выпускается большое количество дополнительных устройств к аппаратуре STU-3. Так, компания «Моторола» изготовляет портативные модели телефонов STU-3 для сотовых систем мобильной связи, но стоимость их около 10 000 $.

В России тоже ведутся подобные работы по массовому внедрению специально разработанной техники в государственные организации и частные фирмы, работающие с ними. Так, на проходившей в 1995 году выставке «Связь-Экспоком» были представлены междугородная АТС **«Фобос-КМ»** и учрежденческая АТС **«Сателлит»**, где циркулирующая информация надежно защищена как техническими, так и криптографическими методами.

Отечественный аналог STU — телефонная система «Гамма», хотя внешне довольно неказиста, но, по словам разработчиков, сравнима по процессорной мощности с пятью «Пентиумами» и обеспечивает практически абсолютную конфиденциальность переговоров.

Разработана аппаратура для закрытия передаваемой информации по каналам факсимильной и телексной связи. Так, «факсовый» шифратор **FSR-2000** подключается между факсимильным аппаратом и розеткой. Шифрующее устройство работает автоматически, при этом специальная функция идентификации (до сотни фамилий и телефонных номеров) позволяет выбрать режим работы под шифрующее устройство адресатов для проведения обмена информацией. Кроме того, аппаратура сообщает о наличии на набранном - номере шифрующего устройства. Габариты изделия не превышают 305x250x64 мм, вес — 2,5 кг. Более поздняя модификация **FSR-3000** использует стандартный алгоритм DES.

Некоторое распространение получили абонентские терминалы, предназначенные для передачи конфиденциальных данных и буквенно-цифровых текстов по телефонной сети общего назначения, а также через УКВ-радиостанцию.

Рассмотрим технические характеристики подобной аппаратуры на примере изделия «Исса». Устройство конструктивно выполнено в корпусе «дипломата» (габариты — 480x340x100 мм), имеет клавиатуру, дисплей,

адаптеры для акустического подключения к трубке ТА. Ввод данных может производиться как с встроенной клавиатуры, так и из внешней ПЭВМ. Скорость передачи данных 600 или 1200 бит/с. Время передачи 2560 знаков не менее 1,5 мин. Аппаратура обеспечивает невозможность прочтения информации в линии связи без знания пароля в течение 2 лет. Длина пароля — 32 знака. Питание возможно как от сети 220 В, так и от встроенного аккумулятора. Вес устройства — не более 7 кг.

Хочется отметить, что, судя по высказываниям американских специалистов подразделения «Группы А» (в АНБ она отвечает за анализ и дешифровку перехваченных сигналов российских радиостанций), в последнее время Соединенным Штатам не удалось раскрыть ни одного из основных российских шифров.

В связи с внедрением техники закрытия телефонных сообщений высокого качества и в коммерческую область успехи аналитического дешифрирования в АНБ этих материалов тоже носят весьма ограниченный характер. В целом с начала 80-х годов XX века четко обозначилась крайне неприятная для промышленных шпионов тенденция: усилия по дешифровке дают все меньше и меньше результатов. Для добывания условной единицы информации приходится затрачивать все больше и больше средств. Как видите, криптозащита — «крепкий орешек» даже для мощных государственных структур.

Помимо перечисленных выше комплексов, которые могут быть использованы только государственными структурами или крупными компаниями связи, аппаратура криптографической защиты выпускается и для индивидуального пользования в виде приставок к ТА. Такие приборы получили название скремблеры. Конечно, степень защиты в этом случае несколько ниже, чем в государственных системах, но все-таки работы промышленному шпиону существенно прибавляется. Действительно, для того чтобы раскрыть смысл защищенного криптографическим способом телефонного разговора, злоумышленнику, как минимум, потребуется:

>• наличие квалифицированного криптоаналитика;

>• редкое, дорогостоящее оборудование;

>• определенное время для расшифровки.

Как известно, криптоаналитики — «товар штучный». Поэтому даже если и удастся найти такого «левого» специалиста, то услуги его буду стоить не просто дорого, а очень дорого. Огромная проблема — добыть соответствующее оборудование, уже не говоря о том, что цена на подобные системы замыкается многими нулями. И наконец, последний фактор может свести на нет все усилия, поскольку к моменту раскрытия сообщения высока вероятность того, что оно уже по всем статьям устарело. Кроме того, при наличии хорошего скремблера момент раскрытия может вообще не наступить.

Принято считать, что скремблеры обеспечивают наивысшую степень защиты конфиденциальности телефонных переговоров. Это действительно так, но при условии, что алгоритм кодирования имеет достаточно высокую криптостойкость. Большим достоинством таких систем является то, что защита обеспечивается на всем протяжении линии связи, в том числе и на самой АТС. Совершенно безразлично, какой аппаратурой перехвата пользуются злоумышленники. Все равно они не смогут в реальном масштабе времени декодировать полученную информацию, пока не раскроют ключевую систему защиты и не создадут автоматический комплекс по перехвату. Впрочем, деяние такого рода уже находится в области «очевидное невероятное». Надо очень сильно «обидеть» какую-нибудь могучую структуру, чтобы она пошла на поистине немереные затраты по созданию подобного комплекса.

К сожалению, помимо явных достоинств применение скремблера для защиты телефонных линий имеет и ряд недостатков. Остановимся на основных из

них.

**Во-первых**, необходимость установки совместимого оборудования у всех абонентов, участвующих в закрытых сеансах связи. Не слишком облегчило проблему и появление так называемых «одноплечевых» скремблеров. В этом случае вместо установки второго прибора у противоположного абонента он устанавливается на городской АТС. Теперь сообщение расшифровывается на середине пути, т. е. закрывается только линия от ТА до станции (зоны А, Б и В), значит, у злоумышленников появляется реальная возможность перехвата информации с телефонной линии партнера. Но самое главное — далеко не все фирмы связи оказывают такого рода услугу, а владелец скремблера становится заложником финансовых аппетитов телефонной компании. И хотя, конечно же, не все учреждения связи в своей тарифной политике обладают такими поистине бандитскими наклонностями, как телефонисты Санкт-Петербурга, и не везде властные структуры дают карт-бланш на беззастенчивое выворачивание карманов у клиентов, все-таки надо помнить, что наши законы, как правило, защищают монополиста от потребителя, а не наоборот. Кроме того, можно серьезно пострадать от неповоротливости служащих телефонной компании при выходе скремблера из строя, а также понести потери от появления третьего лица, знающего о том, что клиент пользуется закрытой телефонной линией и тип аппаратуры криптозащиты.

**Во-вторых**, потеря времени, необходимая в самом начале сеанса связи для синхронизации аппаратуры и обмена ключами. Поэтому при покупке прибора надо обязательно обращать внимание и на эту немаловажную характеристику.

**В-третьих**, временная задержка между моментом передачи и моментом приема речевого сообщения. На людей эмоциональных это действует как сильный раздражающий фактор.

**В-четвертых**, происходит потеря качества сигнала. Узнать человека по голосу при разговоре через защищенную линию совершенно невозможно.

**В-пятых**, невозможность противостоять перехвату речевой информации из помещений в промежутках между разговорами. Телефонная линия используется непостоянно, а большую часть суток находится в «отбое». Следовательно, в эти промежутки времени возможно осуществить перехват речевой информации из помещения, используя проходящие по нему телефонные провода и установленный ТА, например применив устройство типа **Elsy** (см. раздел 1.5). В настоящее время ни один из самых «навороченных» скремблеров не оборудован достаточно надежной системой предотвращения перехвата речевой информации из помещений по телефонной линии, находящейся в «отбое». Таким образом, это техническое средство не является панацеей от всех бед, а защищает только сам телефонный разговор, поэтому должно использоваться в комплексе с другими приборами.

Технические характеристики некоторых приборов отечественного производства приведены в табл. 2.4.3.

Опишем подробнее некоторые модели, наиболее распространенные на потребительском рынке.

**Скремблер SCR-M1.2.** Этот относительно недорогой прибор использует цифровую обработку сигнала для приведения его к виду, удобному для шифрования. Метод шифрации — мозаичный: частотная и временная перестановки. Время задержки — не более 0,45 с. Обеспечивается высокое качество восстановления речи — слоговая разборчивость

**Таблица 2.4.3. Сравнительные характеристики российских скремблеров для зашиты информации в телефонном канале**

Параметры /«Орех-А» /«Базальт» /УЗА /СТА-1000 /SCR-M1.2

Режим работы /Дуплекс /П/дуплекс /П/дуплекс /Дуплекс /Дуплекс

Количество уровней защиты /3 /1 /1 /1 /2
Разрядность ключа /128 /19...16 /16 /До 16 /61
Количество комбинаций /10й /$10^{16}$ ч /$10^{16}$ /$10^{16}$ /2x$10^{25}$
Время установления связи, сек /1...7 /2...8 /8 /Н.д. /Н.д.
Разборчивость речи, % /90 /Н.д. /95 /90 /95
Время задержки сигнала, с /0,32 /0,32 /0,9 /0,32 /0,45
Количество кнопок управления /1 /4 /Н.д. /4 /4
Потребляемая мощность, Вт /10 /Н.д. /Н.д. /6 /10
Габариты, мм /190x290x45 /210x290x45 /Н.д. /330x260x65 /275x290x65
Масса, кг /2 /2,5 /8,2 /3 /3,2

превышает 95 %. Использован довольно удобный алгоритм шифрации, который предполагает метод открытого распределения ключей, что устраняет необходимость в ручном наборе ключей абонентом. Имеется возможность, при надобности, использовать дополнительный семизначный ключ для идентификации собеседника. Общее количество ключевых комбинаций — 2x$10^{25}$. Любопытной особенностью данного прибора является невозможность несанкционированного съема информации с линии даже при наличии у злоумышленника аналогичного изделия (третий скремблер синхронизироваться просто не будет). Внешний вид устройства представлен на рис. 2.4.23.

**Скремблер SCR-M1.2 mini.** Несмотря на практически одинаковое обозначение с предыдущим, представляет собой по сути совершенно новый прибор. От базовой модели оставлен только способ обработки и кодирования сигнала. Сочетает высокое качество работы с малыми габаритами и предельной простотой управления. Особенно удобен для использования в условиях командировок и т. д.

Питание — от сетевого адаптера 9 В или от внешних батарей, потребляемый ток — всего 120 мА. Индикация режимов — световая. Габариты — 115x200x30 мм, вес — 0,8 кг. Цена — даже несколько ниже, чем у базовой модели.

**Многоабонентский скремблер SCR-1.2 multi.** Стоит существенно дороже, зато очень удобен при построении закрытых сетей связи, поскольку специально предназначен для работы в составе офисных мини-АТС типа Hicon, MD110 и т. д. Прибор включается между городской телефонной линией и мини-АТС, обеспечивая работу в закрытом режиме всех телефонных и факсимильных аппаратов в данном офисе. Таким образом, значительно сокращается общее количество скремблеров, поскольку оно зависит не от количества аппаратов, а от количества закрываемых городских телефонных каналов.

Обработка сигнала и алгоритм шифрации такие же, как и у базовой модели. Кроме того, прибор может обеспечить работу по физическим линиям без АТС. Гибкость программного обеспечения позволяет учесть многие пожелания заказчика и гарантирует высококачественную работу с использованием учрежденческих станций практически любого типа.

**Абонентский комплект** «Грот». Реализует новую концепцию защиты речевой и факсимильной информации на участке канала от абонента до городской телефонной станции (рис. 2.4.26). В состав комплекта входят два блока:

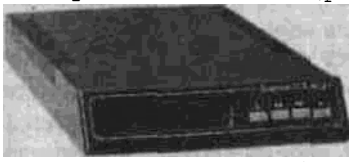


**Рис. 2.4.23. Скремблер SCR-M1.2**

**Рис. 2.4.24. Скремблер SCR-M1.2 mini**

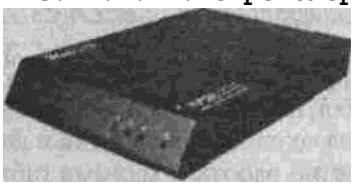


**Рис. 2.4.25. Многоабонентский скремблер SCR-1.2 multi**

**Рис. 2.4.26. Комплект «Грот» и «Грот-С»**

>• скремблер «Грот», устанавливаемый у абонента;

>• скремблер «Грот-С», управляемый дистанционно и устанавливаемый на городской телефонной станции.

Важным преимуществом комплекта является то, что при наличии у противоположного абонента скремблера серии SCR любой модели возможен режим закрытия всего тракта связи между собеседниками. В этом случае «Грот-С» не участвует в сеансе и находится в режиме «обход». Кроме того, данный комплект обладает неплохими потребительскими свойствами, выгодно отличающими его от предшествующих моделей. В частности, сокращено время задержки при обработке речевого сигнала, понижен уровень собственных шумов и улучшена эхокомпенсация. Несомненным достоинством является так же возможность организации уникальной криптографической версии на каждой абонентской линии.

**Скремблер «Орех-А».** Очень удачный и довольно дешевый экземпляр, выпускаемый зеленоградской фирмой «АНКАД». Прибор совершенно не бросается в глаза, поскольку выполнен в виде подставки под ТА, и очень удобен в работе, так как управляется только одной кнопкой. Технические характеристики приведены в таблице 2.4.3, а внешний вид Прибора изображен на рис. 2.4.27. Думаем, достаточно немного проанализировать данные таблицы, чтобы сделать вывод, что это изделие может смело претендовать на оценку одного из лучших по критерию стоимость/эффективность.

**Скремблер-накладка** на телефонную трубку **ASC-2** (рис. 2.4.28). Не обойдены вниманием и те абоненты, у которых по какой-то причине нет постоянного стационарного телефона. Компактное, полностью автономное кодирующее устройство ASC-2 позволяет вести конфиденциальные переговоры с любого случайного телефона, в том числе уличных

Рис. 2.4.27. Скремблер «Орех-А»

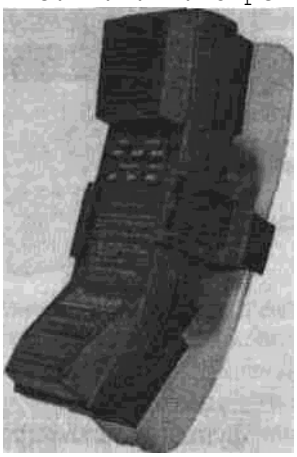


**Рис. 2.4.28. Скремблер-накладка ASC-2**

таксофонов, радиотелефонов и аппаратов сотовой связи. Интересно отметить, что это единственный отечественный скремблер, который защищает как от прямого подслушивания в линии, так и от подслушивая с использованием закладных устройств, установленных непосредственно в ТА, поскольку кодируется сам акустический сигнал. Снабжается специальным ремнем, позволяющим легко крепить его к телефонной трубке.

Прибор имеет следующие технические характеристики. Время полной синхронизации (т. е. установления режима защищенной связи) — 2,5 с. Количество ключей — 13 122, полоса частот — 300...2750 Гц. Питание — от батареи 9 В (типа «Крона»). Габариты — 196x64x53 мм. Вес — 264 г.

Телефонный аппарат-скремблер **Vois Coder 2400** (рис. 2.4.29). Представляет собой систему защиты более высокого уровня, чем все вышеописанные приборы. Конечно, имеет и существенно более высокую стоимость. Предназначен для гарантированной защиты телефонных переговоров от несанкционированного перехвата. Использует алгоритмы шифрования на основе методов линейного и параметрического кодирования. Обеспечивает передачу речевого сигнала по каналам связи в цифровом виде.

**Vois Coder** — это первый в России специализированный цифровой ТА для передачи конфиденциальной информации, обладающий обширным сервисом. Обеспечивает скорость передачи 2400 бит/с в режиме полного дуплекса при использовании помехоустойчивого кодирования и методов защиты информации на основе разграничения доступа. Индивидуальный доступ

**Рис. 2.4.29. Телефон-скремблер Vois Coder 2400**

к защищенному режиму связи производится только после ввода соответствующего пароля с местной энергонезависимой памяти. Переход в защищенный режим и обратно осуществляется простым нажатием клавиши на передней панели. При этом аппарат может работать как напрямую с телефонной сетью, так и с использованием внутриофисной мини-АТС.

Телефон обеспечивает все сервисные услуги современного аппарата, имеет:

>•память на 16 номеров;

>• функцию запоминания последнего, номера;

>• режим громкоговорящей связи;

>• импульсный и тональный набор номера;

>• регулировку громкости и т. д.

Габариты — 240x230x90 мм. Масса — 1,2 кг. По внешнему виду и правилам использования в открытом режиме практически не отличается от стандартного телефона.

В заключение дадим несколько практических советов по выбору скремблера:

**>•** остановитесь лучше на отечественной модели: по степени защиты, техническим характеристикам, а теперь и дизайну они, как минимум, не уступают импортным скремблерам такого же класса, зато прекрасно адаптированы к «особенностям» наших телефонных линий и существенно дешевле;

>• не покупайте совсем дешевые приборы, поверьте — это пустая трата денег, так как в них очень простой алгоритм закрытия сигнала и надо 2—3 мин на адаптацию специальной подслушивающей аппаратуры среднего класса, поэтому такой аппарат защитит только от ревнивой жены или любопытной секретарши;

>• не берите самоделок и «безродные» модели — работа с ними стоит в одном ряду с танталовыми муками, поскольку уже после нескольких сеансов вхождение в синхронизм будет происходить с очень большой задержкой: скремблер — весьма сложный и тонкий прибор, поэтому для его отладки мало «золотых рук», а нужна редкая и дорогая аппаратура;

>• ни в коем случае не афишируйте наличие в вашей организации закрытых каналов связи, тем более никому из посторонних не называйте тип аппаратуры и не демонстрируйте сам прибор, скремблер в перерывах между сеансами лучше держать в сейфе, а установленный стационарно в мини-АТС надо спрятать в запираемый на замок металлический шкаф;

>• практика показывает, что для ведения деловых бесед, а не отдачи приказов или «сброса» факсов необходимо использовать только те модели скремблеров, которые работают в дуплексном режиме и имеют максимально упрощенную систему управления;

>• при выборе конкретной модели не особенно доверяйте рекламе, а лучше посоветуйтесь с нейтральным специалистом.

Теперь несколько слов об обеспечении безопасности телефонов с радиоудлинителями. Всего десять лет назад домашние беспроводные телефоны были в диковинку, теперь они уверенно входят в наши квартиры и офисы, вытесняя своих предшественников, намертво привязанных к телефонной розетке. Перечислять все достоинства таких аппаратов смысла нет — они очевидны. Но, как это часто бывает, достоинства не обходятся

без недостатков. Главная проблема домашних беспроводных радиотелефонов — радиопомехи. Многие слышали «душераздирающие истории» о том, что при включении телефона перестает работать телевизор, притом на самом интересном месте фильма. Но это еще полбеды. Гораздо хуже, когда сигнал вашего радиотелефона перехватят «доброжелатели». Как уже говорилось в разделе 1.5, наличие такого аппарата у поднадзорного лица — голубая мечта любого специалиста по промышленному шпионажу. Существует несколько методов, позволяющих частично решить эту проблему, но мы не будем на них останавливаться, поскольку задача легко решается радикально.

В 1992 году был разработан новый стандарт специально для беспроводной телефонной связи. Он получил название DECT (Digital Enhanced Cordless Telecommunications, Цифровая усовершенствованная беспроводная связь). Кратко охарактеризовать этот стандарт можно так: «младший брат GSM». Хотя несколько отличий все-таки есть, но, по сути, это очень близкие технологии.

Мощность передатчиков в трубке и базе очень низкая (10 мкВт), что, с одной стороны, повышает скрытность и гарантирует безопасность для здоровья людей, но с другой — ограничивает дальность действия (около 50 м в помещении). Но, конечно, главные достоинства стандарта DECT, как и его «старшего брата», заключаются в высоком качестве связи и ее надежной защищенности от прослушивания и «подсадок» от других телефонов. Внешне аппарат

**Рис. 2.4.30. Аппарат Spree стандарта DECT**

**Рис. 2.4.31. Телефонный аппарат Samsung стандарта DECT**

стандарта DECT очень напоминает обычный домашний радиотелефон и совершенно не отличается от последнего по правилам пользования. Стоимость подобного устройства, конечно, выше, чем стандартного, но комфорт и безопасность вообще стоят дорого.

Имеются в продаже и более «навороченные» экземпляры. В качестве примера такого устройства можно привести аппарат фирмы «Сименс» **Gigaset** серии 2000. Данный прибор обладает хорошим качеством передачи речи и высоким уровнем защиты как от подслушивания, так и от несанкционированного доступа. Используется стандарт DECT/GAP (GAP — метод радиопередачи в стандарте DECT, не ориентированный на технику конкретного изготовителя). Имеется память на 10 номеров, функции повторного набора 5 последних номеров и экстренного вызова, функция записной книжки, громкоговорящий прием. Переносной телефон очень легок и компактен — всего 165 г вместе с аккумулятором.

Но самое интересное — имеется возможность расширения комплекта до 6 переносных телефонов с функцией связи между ними. Правда, возможно одновременное ведение внутреннего разговора только между двумя переносными телефонами, но при этом с третьего телефона можно вести один внешний разговор. Можно осуществить общий внутренний вызов или дать уведомление о поступлении внешнего вызова абоненту во время ведения им внутреннего разговора. Телефон совместим почти со всеми типами мини-АТС. Дальность связи на открытой местности — до 300 м и до 50 м — в здании. Способ набора номера: импульсный или тональный. При использовании устройства беспроводного подключения **Gigaset 1000TA**, сама база тоже становится переносной и питается от никель-кадмиевого аккумулятора. Можно включить в комплект и цифровой автоответчик. Внешний вид аппаратов стандарта DECT приведен на рис. 2.4.30 и 2.4.31.

Наша информация о системах криптозащиты будет неполной, если не поднять вопрос, который очень часто задают начальники достаточно солидных служб безопасности: «Как защитить от прослушивания УКВ-радиосвязь, используемую для диспетчерских нужд при охране объектов, сопровождении транспортных средств, проведении каких-либо мероприятий? Доводим до сведения заинтересованных лиц, что для этих целей разработано несколько моделей специальных скремблеров. Большинство из них реализует частотную инверсию сигнала. Все они имеют очень близкие параметры, совсем невысокую стоимость и, как правило, устанавливаются прямо на корпусе радиостанции.

Одними из первых на рынке появились приборы фирмы Selectone, такие, как SS-20 и более поздняя модель **ST-022.** Скремблеры работают в диапазоне частот 300...2400 Гц и обеспечивают инверсию сигнала относительно 8

номиналов частот. Габариты — 39x21x14 мм.
Скремблеры фирмы Midian типа **VPV** обладают схожими параметрами, но имеют уже 15 частот инверсии.
Более сложное преобразование сигнала происходит в разработанных НТЦ «ИНТЕРВОК» скремблерах типа **«Сонет».** Здесь спектр речевого сигнала делится на две части, каждая из которых разворачивается вокруг своих средних частот. Приборы имеют очень малые размеры (15x15x6,5 мм) и легко устанавливаются внутри корпуса практически любых радиостанций.
Таким образом, для пользователя на рынке спецтехники представлен очень широкий выбор. Вместе с тем желающим приобрести средства УКВ-связи, обеспечивающие надежную защиту передаваемой информации, хотелось бы все-таки рекомендовать при закупке подходить к проблеме комплексно, т. е. на начальном этапе четко определиться с уровнем необходимого закрытия канала. Следует помнить — **аналоговые скремблеры никогда не обеспечат защиту** от преднамеренного прослушивания переговоров, если злоумышленником используется специальный комплекс радиоразведки. При этом финансовые затраты лиц, ведущих съем информации, не будут являться для них препятствием (стоимость хорошей профессиональной аппаратуры для перехвата сигнала закрытого таким скремблером или совершенно открытого не изменится). Для по-настоящему надежной защиты информации в радиоканалах необходимо использовать аппаратуру, где передача сигнала осуществляется в цифровой форме. То есть в действительно важных случаях следует применять существенно более дорогие цифровые радиостанции или использовать цифровые скремблеры для аналоговых связных систем. Подобные устройства уже выпускаются рядом организаций.

### 2.4.5. Защита от пиратских подключений

Отдельная, но очень актуальная проблема — борьба с лицами, незаконно подключившимися к чужим телефонным сетям и использующими их для своих целей, например для звонков в дальнее зарубежье. На Западе называют таких телефонных пиратов фрикерами. Общественность уже свыклась с мыслью о том, что без хакеров нет Интернета. Про них слагают легенды и небылицы, создавая вокруг сетевых взломщиков ореол романтики. О фрикерах информации намного меньше. Телефонные компании не заинтересованы в том, чтобы подобные случаи предавались огласке. С широким распространением радиотелефонов различного типа (от сотовых до элементарных домашних «радиоудлинителей») эта проблема еще более обострилась. Некоторые специалисты считают, что данные вопросы напрямую не связаны с защитой информации (скорее, это защита кошелька), но проблема стоит того, чтобы ее рассмотреть более подробно.
Традиционно все способы противодействия делят на две основные группы:
>• организационные;
>• технические.
Под организационными способами понимается комплекс мер по регламентированию и контролю за использованием телефонной линии. Они проводятся (или, по крайней мере, должны проводиться) как работниками линейных узлов связи, так и индивидуальными абонентами АТС. Особенно большой эффект от организационных мер получают предприятия и организации, на балансе которых имеется достаточно много городских телефонных линий.
Под техническими способами противодействия понимается применение специальных устройств защиты, ограничивающих возможности нелегальных абонентов по доступу к линиям связи, особенно междугородным.
По способу воздействия на телефонные линии технические способы подразделяются на:
>• пассивные;
>• активные.
Пассивные устройства защиты предназначены только для регистрации факта

подключения и самовольного использования линии. Они не вмешиваются в сам сеанс связи, а только помогают владельцу линии оперативно среагировать на действия по ее «самозахвату».
Активные устройства защиты предусматривают вмешательство в процесс установления и проведения связи с целью предотвратить реальные финансовые затраты в случаях самовольного подключения. Основные способы противодействия приведены на рис. 2.4.32.
Так, для защиты проводных телефонных линий разработан совмещенный индикатор подключения и обрыва линии, принципиальная схема которого приведена на рис. 2.4.33. В состав схемы входят:
>• диодный мост для подключения к линии без учета полярности — VD1—
**>• датчик напряжения — VD5, R1, VD6, R2, VD7, C1, DD1.1;**
>• фильтр вызова АТС (25 Гц) — R3, C2, DD1.2;
>• инверторы — DD1.3, DD2.2;
>• генератор 2,5 кГц — DD1.4, DD2.1, R4, C3;

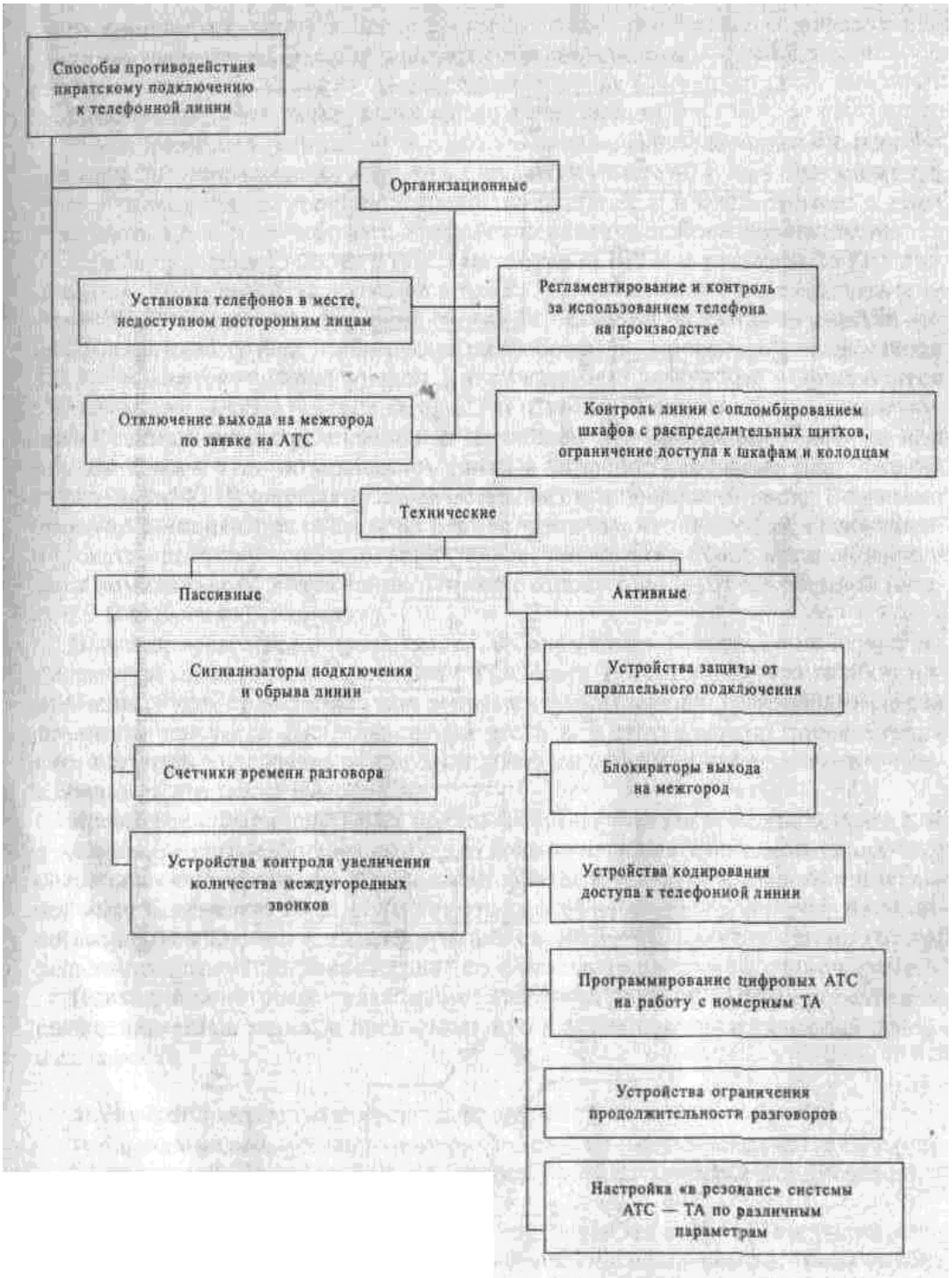



**Рис. 2.4.32. Способы противодействия пиратскому подключению к линии**

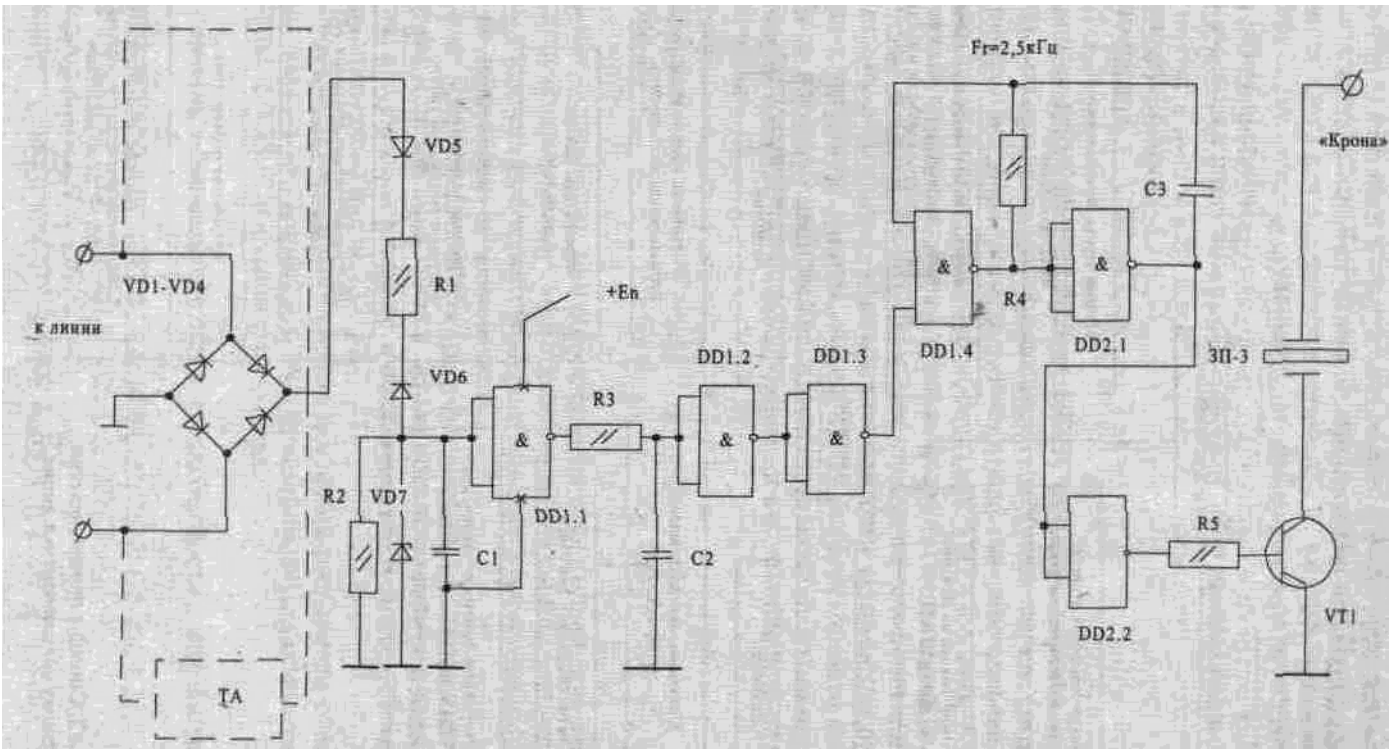



**Рис. 2.4.33. Совмещенный индикатор подключения и обрыва линии**

**>• ключ - R5, VT1;**

>• звуковоспроизводящий элемент (пьезоизлучатель) — ЗП-3.

Принцип работы схемы заключается в следующем.

В исходном состоянии блок индикатора подключается параллельно используемому ТА. При наличии в линии напряжения свыше 40 В на входе элемента DD1.1 присутствует уровень логической единицы, и в соответствии с этим генератор 2,5 кГц не работает. Устройство находится в режиме ожидания.

При поступлении вызова с АТС (амплитудой 100 В и частотой 25 Гц) специально рассчитанная цепочка фильтра R3, С2 не позволяет переключить элемент DD1.2 и включить звуковой сигнал ЗП. Если же на каком-то участке линии была снята трубка (либо произошел обрыв) более чем на 1 с, на выходе DD1.1 появится нулевой уровень, и с указанной задержкой переключится DD1.2. Далее включится генератор 2,5 кГц, который подаст непрерывный звуковой сигнал, предупреждающий о пиратском использовании телефона или обрыве линии. При возвращении линии в исходное состояние (напряжение стало более 40 В) индикатор вновь переходит в ждущее состояние. Возможна доработка индикатора схемой на основе триггера, что позволит «задокументировать» попытку использования (обрыв) линии даже после установления в сети номинального напряжения. Питание индикатора — от встроенной батареи 9 В («Крона», «Корунд»).

Благодаря высоким номиналам R1, R2 индикатор абсолютно не влияет на параметры линии (в соответствии с ГОСТом). Естественно, что прибор непременно будет срабатывать при подъеме трубки (ведение разговора) и самим хозяином телефона. Для ликвидации этого недостатка можно порекомендовать встроить выключатель или выполнить индикатор в виде заглушки, подключаемой к розетке вместо ТА.

Кроме всех видов пиратских подключений на участке проводной связи для домашних радиотелефонов характерно подключение и в зоне радиоканала. Эту операцию очень легко проделать, когда в режиме «отбоя» трубка потенциальной жертвы не лежит на базе. Количество жалоб на деяния

такого рода постоянно возрастает. Однако соответствующие службы АТС практически не готовы решать проблему противодействия телефонному пиратству на радиочастоте.
Правда, в некоторых типах радиотелефонов, появившихся на российском рынке, защита от пиратов предусмотрена, в основном применены два основных способа:
>• скачкообразное изменение частоты;
>• наличие индивидуального номера у каждой зарегистрированной на базе (стационарном блоке) трубки, по которому осуществляется ее опознавание.
Однако «черный» рынок мгновенно отреагировал появлением так называемых трубок-сканеров, сводящих на нет эти способы защиты. Такая трубка

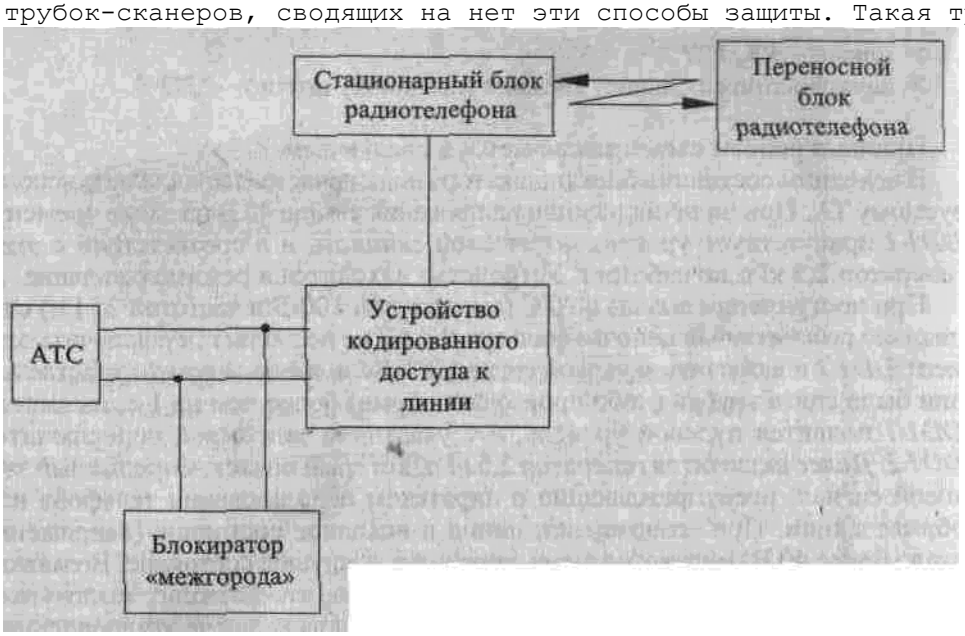



**Рис. 2.4.34. Схема защиты домашнего радиотелефона**

легко позволяет отследить как скачки частоты (ибо количество фиксированных частот весьма ограничено), так и подобрать индивидуальный номер методом перебора.
Единственным на сегодняшний день реальным способом борьбы с этими приборами (без изменения принципиальной схемы самого радиотелефона) является установка блокиратора «межгорода» и блока дополнительного кодирования линии. При достаточно частой смене кода вероятность того, что пираты будут анализировать этот код, набираемый вручную, и подбирать ключи очень мала. Очевидно, что им легче просто перебраться на какую-нибудь незащищенную линию. На рис. 2.4.34 приведена структурная схема защиты домашнего радиотелефона. Кстати, установка абсолютного блокиратора «межгорода» (т. е. блокиратора, который можно отключить, лишь находясь в помещении, где он установлен) позволяет на все 100 % гарантировать отсутствие чужих счетов за дорогостоящие междугородные переговоры с защищенного телефона.
В качестве примера практической реализации блокиратора «межгорода» можно привести устройство **БМ-01** (рис. 2.4.35), которое совершенно не бросается в глаза, поскольку изготовлено в форме телефонной розетки. В виде исключения приведем стоимость этого прибора по городу Москва — на июль 1999 года она составляла всего 4 $! Если сравнить эту сумму с размерами возможного счета за международные переговоры, то вывод напрашивается сам собой.
Имеются в продаже и устройства, обеспечивающие кодирование доступа к линии. Например, очень недорогое многофункциональное устройство защиты телефонной линии «Вьюга-4» (рис. 2.4.36). Изделие устанавливается в ли-

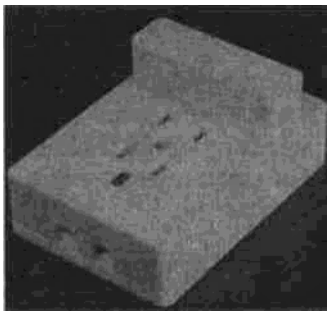


**Рис. 2.4.35. Блокиратор «межгорода» БМ-01**

**Рис. 2.4.36. Многофункциональное устройство защиты «Вьюга-4»**

нии городских и офисных АТС напряжением от 30 до 75 В. Прибор выполнен в виде отдельного блока и рассчитан для установки на стене, он снабжен колодками для подключения входной и выходной линий с соблюдением полярности. Устройство распознает постороннего пользователя при отсутствии набора специального кода, предшествующего набору номера, и блокирует линию. Код программируется самим абонентом при помощи ТА. Память устройства хранит два кода для разрешения пользования городской и междугородной связью. Длина каждого кода доступа — от 1 до 4 цифр. Питание — от встроенной батареи. Управление изделием осуществляется в импульсном режиме телефона, если аппарат работает в тональном режиме, то на время набора кодов и программирования следует перевести телефон в импульсный режим. Однако блокировка посторонних звонков осуществляется в любом режиме. Габариты —104x53x28 мм.

Помимо защиты линии от доступа посторонних абонентов устройство работает как индикатор: дает предупредительный звуковой сигнал, слышимый в помещении и телефонной трубке (во время разговора) при возникновении тревожной ситуации. При этом загоревшиеся светодиоды оповещают о виде происшедшего нарушения — разрыв линии или изменение ее параметров.

### 2.4.6. Технические средства пространственного и линейного зашумления

По принципу действия все технические средства пространственного и линейного зашумления можно разделить на три большие группы.

1. Средства создания акустических маскирующих помех:
>• генераторы шума в акустическом диапазоне;
>• устройства виброакустической защиты;
>• технические средства ультразвуковой защиты помещений.
2. Средства создания электромагнитных маскирующих помех:
>• технические средства пространственного зашумления;
>• технические средства линейного зашумления; которые, в свою очередь, делятся на средства создания маскирующих помех в коммуникационных сетях и средства создания маскирующих помех в сетях электропитания.
3. Многофункциональные средства защиты. Рассмотрим их более подробно.

СРЕДСТВА СОЗДАНИЯ АКУСТИЧЕСКИХ МАСКИРУЮЩИХ ПОМЕХ

**Генераторы шума в акустическом диапазоне**

Генераторы шума в речевом диапазоне получили достаточно широкое распространение в практике защиты информации. Они используются для защиты от несанкционированного съема акустической информации путем маскирования непосредственно полезного звукового сигнала. Маскирование

проводится «белым» шумом с корректированной спектральной характеристикой.
Примерный вид структурной схемы источника акустического шума приведен на рис. 2.4.37. Конструктивно аппаратура включает блок формирования и усиления шумового сигнала и несколько акустических излучателей.
В качестве примера таких систем могут служить генераторы **Sond Press и WNG-023.**
**Sond Press** — генератор акустического шума с вынесенными источниками излучения.
**Основные технические характеристики**
Мощность шума (max)..... 2 Вт
Спектральная мощность шума..... 0,25 мВт/Гц
Срез спектра шума в НЧ-области..... (<2 КГц)—8 дБ/окт.
Полоса равномерной плотности шума ..... 2 кГц...10 кГц
Дополнительный подъем ВЧ ..... +6 дБ/окт.
Габариты (две колонки) ..... 80x100x155 мм
В некоторых случаях наличие нескольких излучателей необязательно. Тогда используются компактные генераторы со встроенной акустической системой, например WNG-23.
**WNG-023** — акустический генератор «белого», шума.

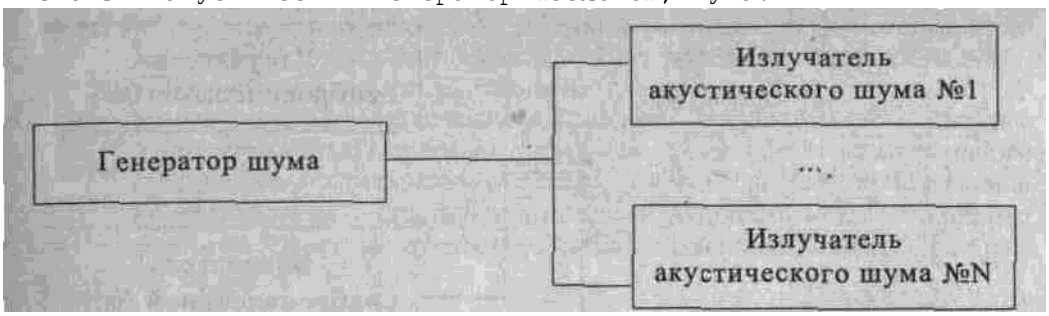



**Рис. 2.4.37. Структурная схема источника акустического шума**
**Основные технические характеристики**
Полоса акустической помехи-»..... 0,1...12 кГц
Вид помехи.....«белый» шум
Излучаемая мощность ..... до 1 Вт
Встроенный аккумулятор (в комплект входит зарядное устройство)
Питание..... 220 В/9 В
Габариты ..... 98x71x30 мм
Главный недостаток применения источников шумов в акустическом диапазоне — это невозможность комфортного проведения переговоров. Практика показывает, что в помещении, где «ревет» генератор шума, невозможно находиться более 10... 15 минут. Кроме того, включается «человеческий фактор» — собеседники, сосредоточившись на разговоре, забывают о безопасности и автоматически начинают пытаться перекричать средство зашиты, снижая эффективность его применения. Поэтому подобные системы, как правило, применяются для дополнительной защиты дверных проемов, межрамного пространства окон, систем вентиляции и т. д.
**Устройства виброакустической защиты**
Наиболее эффективным средством защиты помещений, предназначенных для проведения конфиденциальных мероприятий, от съема информации через оконные стекла, стены, системы вентиляции, трубы отопления, двери и т. д. являются устройства виброакустической защиты. Данная аппаратура позволяет в некоторых случаях предотвратить прослушивание с помощью проводных микрофонов, звукозаписывающей аппаратуры, радиомикрофонов и электронных стетоскопов, систем лазерного съема акустической информации с окон и т. д. Противодействие прослушиванию обеспечивается внесением виброакустических шумовых колебаний в элементы конструкции здания.

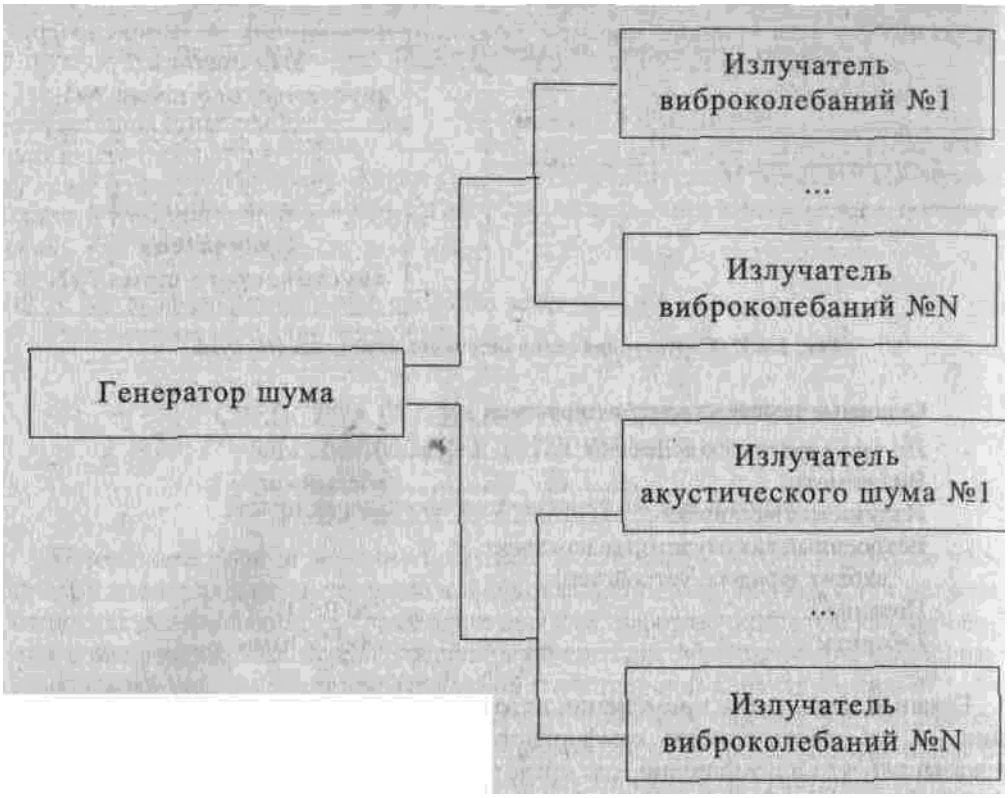



**Рис. 2.4.38. Структурная схема устройства виброакустической защиты**

Типовая структурная схема устройства виброакустической защиты приведена на рис. 2.4.38. Конструктивно аппаратура включает блок формирования и усиления шумового сигнала и несколько акустических и виброакустических излучателей.

Генератор формирует «белый» шум в диапазоне звуковых частот. Передача акустических колебаний на ограждающие конструкции производится при помощи пьезоэлектрических (на основе пьезокерамики) или электромагнитных вибраторов с элементами крепления. Конструкция и частотный диапазон излучателей должны обеспечивать эффективную передачу вибрации. Вибропреобразователи возбуждают шумовые виброколебания в ограждающих конструкциях, обеспечивая при этом минимальный уровень помехового акустического сигнала в помещении, который практически не влияет на комфортность проведения переговоров.

Предусмотренная в большинстве изделий возможность подключения акустических излучателей позволяет «зашумлять» вентиляционные каналы и дверные тамбуры. Как правило, имеется возможность плавной регулировки уровня шумового акустического сигнала.

Стоимость комплекта в зависимости от модели может составлять от 200 до 3000 $. Рассмотрим наиболее известные виброакустические генераторы, представленные на российском рынке.

**ANG OOPS** —устройство защиты акустики помещений. Оптимальный режим защиты может быть создан при помощи двух видов вибродатчиков, акустических систем, суммарным количеством до 36, которые подключаются к 12 независимым усилителям с регулируемой мощностью и с возможностью визуального контроля уровня. Наличие встроенного и выносного микрофонов с регулируемой чувствительностью позволяет автоматически включать и выключать усилители мощности при изменениях уровня акустического сигнала. Внешний вид прибора показан на рис. 2.4.39.

**Основные технические характеристики**

Максимальный уровень громкости защищаемой речевой информации, не более

..... 80 дБ
Полоса частот сигналов защиты ..... 0,04...15кГц
Количество усилителей мощности ..... 12
Сопротивление нагрузки усилителя мощности..... 8 Ом
Эффективный радиус вибропреобразователя ТК1..... 1,5 м
вибропреобразователя ТК3..... 4,3 м
Питание..... 220 В
Габариты:
электронного блока ..... 230x195x63 мм
вибропреобразователя ТК1..... 10x55 мм
вибропреобразователя ТК3..... 120x55 мм
МОДИФИКАЦИИ:
**ANG 007SA** — автономный вариант с дополнительным комплектом батарей (время непрерывной работы — 10ч);
**ANG 007SM** — модернизированный вариант по индивидуальному заказу;
**ANG 007SL** — вариант «Люкс» с улучшенным дизайном.
**NG-502M** — генератор виброакустического шума.
**Основные технические характеристики**
Максимальный уровень громкости
защищаемых речевых сообщений, не более..... 75 дБ
Полоса частот сигнала защиты..... 0,2...15 кГц
Количество датчиков..... до 12
Радиус действия одного датчика ..... 1,5 м
Габариты:
блок-генератора..... 205x60x155 мм

**Рис. 2.4.39. Устройство защиты ANG 007S**

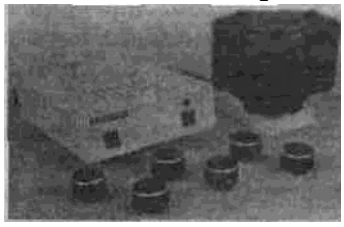


**Рис. 2.4.40. Генератор виброакустического шума NG-502M**

датчика..... 32x21 мм
Питание..... 220 В, 50 Гц
Внешний вид прибора представлен на рис. 2.4.40.
**Radel 01** — генератор виброакустического шума. Это устройство (рис. 2.4.41) представляет собой цифровой двухканальный генератор «белого» шума. Регулировка уровня шума в каждом из каналов осуществляется независимо.
**Основные технические характеристики**
Выходная мощность
каналы А и В ..... 3 Вт
Полоса излучаемых частот ..... 200...12 000 Гц
Напряжение питания..... 12 В
Габариты
генератора (электронный блок)..... 120x90x60 мм
контактных излучателей для установки
на стены ..... 30x34 мм

на окна ..... 30x28 мм

**RNG-01** — генератор акустического «белого» шума.

**Основные технические характеристики**

Диапазон частот..... 100...15 000 Гц
Мощность (max) выходного сигнала ..... 4 Вт
Питание ..... 220 В, 50 Гц
Потребляемая мощность ..... 40 Вт
Габариты ..... 140x127x40 мм

В комплект поставки входят 6 пьезовибраторов с элементами крепления на стены, стекла, трубы и две акустические колонки.

**SPP-4** — генератор виброакустического шума. Особенностью прибора является генерация шума с автоматически регулируемым уровнем, зависящим от акустического фона помещения. Прибор имеет микропроцессорное управление и многофункциональный индикатор уровня. Три независимых канала акустической защиты помещения. Кроме того, он может быть подключен к телефонной линии для создания линейного зашумления. Внешний вид устройства приведен на рис. 2.4.42.

К прибору можно подключить:

>• 20 пьезоизлучателей (по 10 к каждому из каналов А и В);
>• 1 вибрационный излучатель типа «TRN-2000» или 2 акустических излучателя типа «OMS-2000» (или аналогичных) к каналу С.
>• Каждый из трех каналов может работать в одном из трех режимов генерации шума:
>• нормальный режим «белого» шума;
>• режим «белого» шума со случайной амплитудой;
>• режим «белого» шума с автоматическим управлением уровня шума.

**Основные технические характеристики**

Спектр акустического шума прибором по
каналам А, В, С и телефонной линии ..... 200 Гц...6,3 кГц
Максимальный уровень шума (амплитудное значение) на выходе:
каналов А и В ..... 15В
канала С..... 2,5В
телефонного канала..... 3 В
Питание..... 220 В, 50 Гц

VAG-6/6 — виброакустический генератор.

**Основные технические характеристики**

Максимальное количество преобразователей..... 6
Максимальное количество акустических колонок..... 6
Требуемый импеданс нагрузки на выходе акустического канала, не менее..... 16 Ом

**VNG-006** — устройство защиты помещений от утечки информации по виброканалам.

**Рис. 2.4.41. Генератор виброакустического шума Radel 01**

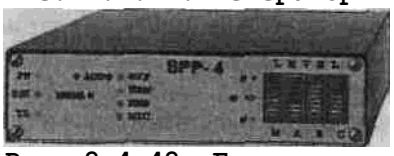



**Рис. 2.4.42. Генератор виброакустического шума SPP-4**

Комплект поставки предусматривает все необходимые установочные элементы для монтажа вибропреобразователей. Внешний вид устройства приведен на рис. 2.4.43.

**Основные технические характеристики**

Максимальный уровень громкости защищаемых речевых сигналов, не более ..... 75дБ
Полоса частот сигнала защиты ..... 0,2...15 кГц
Количество вибропреобразователей ..... 6...12
Эффективный радиус действия одного вибропреобразователя кирпичная стена..... 2,5 м
бетонная стена..... 3 м
Параметры выхода на акустическую систему мощность ..... 3 Вт
импеданс ..... 4...8 Ом
Питание..... 220 В ±10%, 50 Гц

**«Барон»** — комплекс виброакустической защиты. Основные достоинства прибора:

>• возможность формирования помехового сигнала от различных внутренних и внешних источников и их комбинаций. Внутренние источники — генератор шума, 3 независимых радиоприемника. За счет их микширования значительно уменьшается вероятность очистки зашумленного сигнала. Кроме того, наличие линейного входа позволяет подключать к комплексу источники специального помехового сигнала повышенной эффективности;

>• одним прибором можно защитить помещения большой площади различного назначения (конференц-залы и т. п.);

**>•** возможность регулировки спектра помехового сигнала для повышения эффективности наведенной помехи с учетом особенностей используемых вибро- и акустических излучателей и защищаемых поверхностей;

>• наличие 4 независимых выходных каналов с раздельными регулировками для оптимальной настройки помехового сигнала для различных защищаемых поверхностей и каналов утечки;

>• достижение максимальной эффективности подавления при минимальном паразитном акустическом шуме в защищаемом помещении за счет выше перечисленных возможностей настройки комплекса;

>• возможность подключения к каждому выходному каналу различных типов вибро- и акустических излучателей и их комбинаций за счет наличия низкоомного и высокоомного выходов. Это также позволяет использовать комплекс для замены морально устаревших или вышедших из строя источников помехового сигнала в уже развернутых системах виброакустической защиты без демонтажа и замены установленных виброакустических излучателей;

>• наличие системы беспроводного дистанционного включения комплекса.

Внешний вид устройства приведен на рис. 2.4.44.

**Основные технические характеристики:**

Выходная мощность ..... 15 Вт на 4 канала
Количество полос регулировки по частоте..... 3 (250, 1000,4000 Гц)
Диапазон частот усилителей..... 150 Гц...15 кГц
Источники помехового сигнала
внутренние ..... 3 радиоприемника FM-диапазона, 1 генератор шума
внешний ..... через линейный вход
Дальность действия ДУ ..... 30м
Питание ..... 220 В, 50 Гц

**«Соната-АВ»** — генератор виброакустического шума. Состоит из двух независимых генераторов шума, каждый из которых может быть оперативно

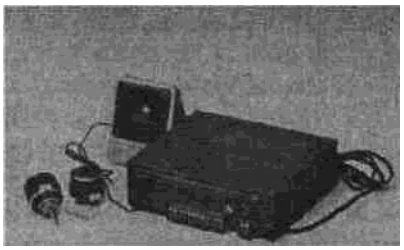


**Рис. 2.4.43. Устройство защиты помещений VNG-006**

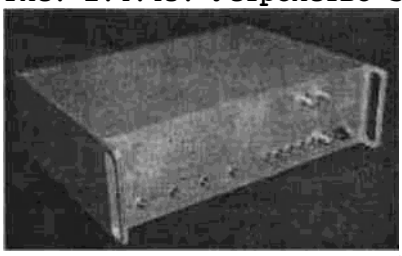


**Рис. 2.4.44. Комплекс виброакустической защиты «Барон»**

настроен на выдачу либо аудио-, либо вибропомехи калиброванной интенсивности. Внешний вид прибора и его излучателей приведен на рис. 2.4.45.

«Соната-АИ» — акустический излучатель;

«Соната-ВИ» — вибрационный излучатель.

**Основные технические характеристики**

Количество независимых каналов..... 2

Максимальное количество виброизлучателей типа ВИ-45х30 на одном выходе ..... 6

типа SB66 (8 Ом) на одном выходе..... до 8

Размах напряжения

на виброизлучателе, не менее..... 100 В

на аудиоизлучателе, не менее..... 1В

Питание ..... 220 В, 50 Гц

Продолжительность непрерывной работы .....до 24 ч

Габариты основного блока.....135х65х155 мм

**«Фон-В»** — система виброакустического зашумления. Используемые в системе генератор ANG-2000, вибродатчики TRN-2000 и TRN-2000M и оригинальные металлоконструкции для крепления вибродатчиков обеспечивают эффективное зашумление строительных конструкций. Монтаж и демонтаж системы осуществляется без повреждения строительных конструкций и элементов отделки интерьера. Внешний вид системы приведен на рис. 2.4.46.

**Основные технические характеристики**

Диапазон частот.....250...5000 Гц

Радиус действия вибродатчика, не более ..... 5 м

Площадь помещения, защищаемая системой ..... до 25 кв. м

Возможность расширения .....до 36 кв. м

Количество в упаковке и вес

«Фон-В1» .....1 шт. 14кг

«Фон-В2» .....2шт. по 12кг

Минимальное время монтажа/демонтажа

системы силами трех человек, не более ..... 30 мин

Монтаж системы виброакустического зашумления осуществляется достаточно просто. Главная проблема заключается в определении нужного количества датчиков и их взаимного расположения на ограждающей конструкции. Дело в том, что приводимые в технических характеристиках площади, перекрываемые одним излучателем, достаточно условные, а такие параметры, как материал (из которого изготовлена стена, дверь, потолок и т. д.), толщина

**Рис. 2.4.45. Генератор виброакустического шума «Соната-АВ»**

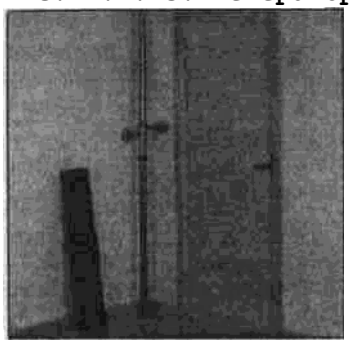


**Рис. 2.4.46. Система виброакустического зашумления «Фон-В»**

конструкции, наличие полостей, качество крепления оказывают большое влияние на эффективность зашумления.

В связи с высокой стоимостью генераторов шума нежелательно приобретение лишнего оборудования, поэтому целесообразно проводить предварительные измерения параметров ограждающих конструкций и только после этого определять необходимый тип генератора и количество датчиков, а также места их расположения. Ясно, что работы такого рода смогут выполнить только квалифицированные специалисты. После завершения монтажных работ целесообразно осуществлять контроль эффективности системы пространственного и линейного зашумления. При этом надо ориентироваться на то, что восстановить перехваченное сообщение практически невозможно, если уровень помехи более чем в 10 раз превышает уровень сигнала во всем частотном диапазоне (отношение сигнал/помеха менее -20 дБ).

**Технические средства ультразвуковой защиты помещений**

Они сравнительно недавно появились в продаже, но зарекомендовали себя как надежные средства технической защиты акустической информации. Отличительной особенностью этих средств является воздействие на микрофонное устройство и его усилитель достаточно мощным ультразвуковым сигналом (группой сигналов), вызывающим блокирование усилителя или возникновение значительных нелинейных искажений, приводящих в конечном счете к нарушению работоспособности микрофонного устройства (его подавлению).

Поскольку воздействие осуществляется по каналу восприятия акустического сигнала, то совершенно не важны его дальнейшие трансформации и способы передачи. Акустический сигнал подавляется именно на этапе его восприятия чувствительным элементом. Все это делает комплекс достаточно универсальным по сравнению с другими средствами активной защиты.

При более-менее кратковременном использовании практически не происходит существенного снижения эргономических характеристик помещения. Рассмотрим пример такого изделия.

«Завеса» — комплекс ультразвуковой защиты акустических сигналов.

В минимальной комплектации обеспечивает защиту в объеме до 27 куб. м Стандартная конфигурация комплекса — двуканальная. При необходимости он

имеет возможность наращивания до 4, 6, 8 и т. д. канальных версий.
Однако ультразвуковые комплексы на один-два порядка дороже своих акустических аналогов и имеют небольшой радиус действия.
Внешний вид комплекса представлен на рис. 2.4.47.
Информация для радиолюбителей. На рис. 2.4.48, а представлена принципиальная схема простейшего генератора шума, способного «закрыть» весь диапазон звуковых волн.
Непосредственно генератор выполнен на транзисторах VT1 и VT2 (могут быть марки КТ805А, КТ805А, Б или из серии КТ601). Амплитуда шумовой составляющей регулируется потенциометром R4. Формируемый сигнал через разделительный конденсатор С3 подается на вход усилителя модулятора (база транзистора VT3). В исходном состоянии этот транзистор закрыт напряжением, поступающим на его эмиттер с делителя на резисторах R12, R13 через R11, R9. Конденсатор С5 при этом заряжен до напряжения, запирающего транзистор.
При замыкании тумблера К1.1 (вынесен за пределы платы и может быть установлен в любом удобном месте) конденсатор С5 быстро разряжается через резистор R7. Транзистор VT3 при этом открывается, и появляется на его выходе усиленный шумовой сигнал. Открытое состояние транзистора будет поддерживаться до тех пор, пока тумблер замкнут. При размыкании тумблера конденсатор С5 вновь начинает заряжаться, что приводит к запиранию транзистора VT3. Резонансный контур L1, С4, включенный в цепь коллектора VT3, позволяет подобрать полосу частот, необходимую для «перекрытия» спектра маскируемого сигнала. На транзисторе VT4 собран согласующий усилитель.

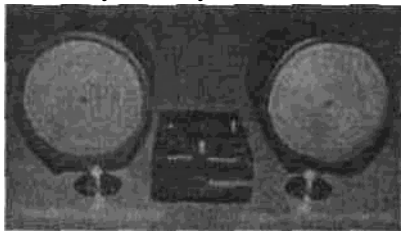


**Рис. 2.4.47. Комплекс ультразвуковой защиты помещений «Завеса»**

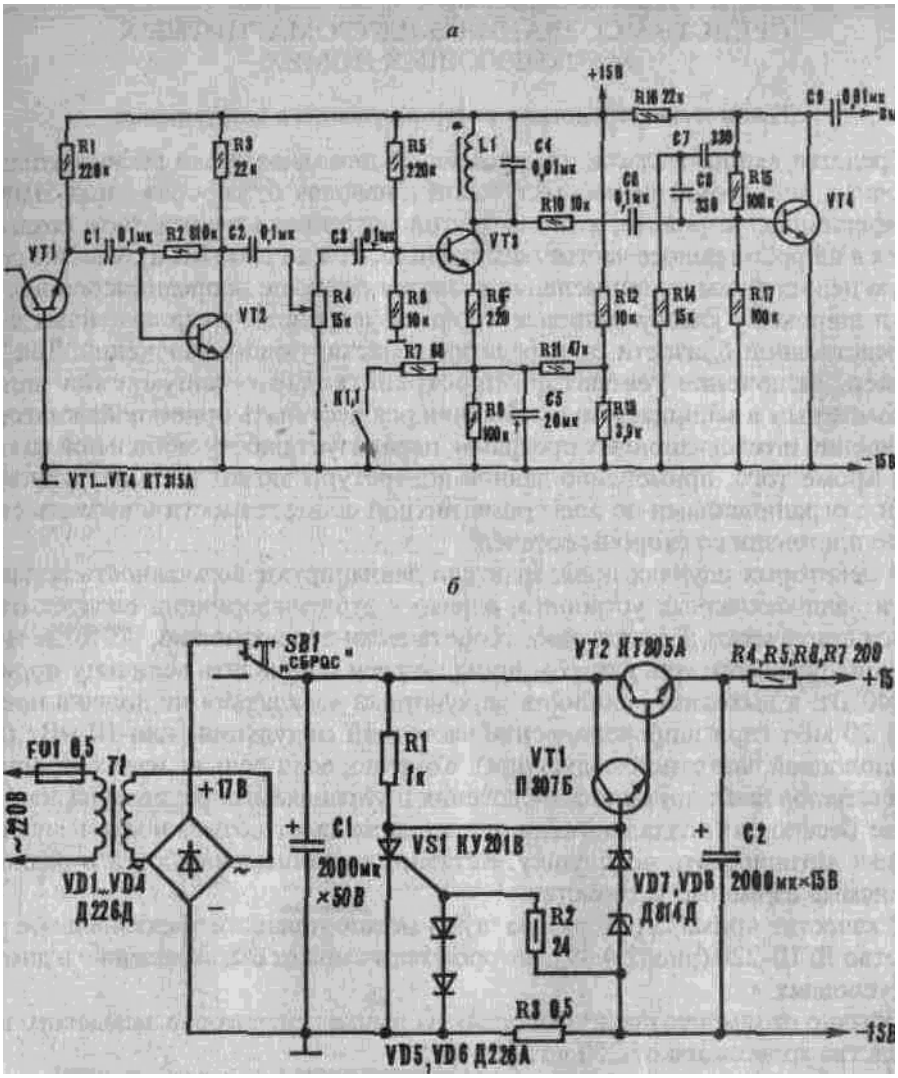



**Рис. 2.4.48. Принципиальная схема источника маскирующих помех:**
а — генератор «белого» шума и усилитель-модулятор; б — блок питания генератора

Для подачи питающего напряжения можно использовать стандартный источник питания или сделать его самому, взяв за основу схему, приведенную на рис. 2.4.48, б.

СРЕДСТВА СОЗДАНИЯ ЭЛЕКТРОМАГНИТНЫХ МАСКИРУЮЩИХ ПОМЕХ

**Технические средства пространственного зашумления**

Средства данного класса предназначены для маскировки информативных побочных электромагнитных излучений и наводок от персональных ЭВМ и периферийных устройств, а также другой оргтехники посредством создания помех в широкой полосе частот (как правило, от 1 до 1000 МГц). Однако серьезным недостатком их применения является создание непреднамеренных помех и широкому классу радиоэлектронных устройств, расположенных в непосредственной близости от передатчика маскирующих излучений. Так, например, включение генератора пространственного зашумления делает невозможным в защищаемом помещении осуществлять прием пейджинговых сообщений и телевизионных программ, парализует работу мобильной связи и т. д. Кроме того, применение данной аппаратуры может быть затруднено в связи с ограничениями по электромагнитной совместимости и вызвать серьезные претензии со стороны соседей.

В некоторых случаях производители декларируют возможность подавления и радиозакладных устройств, однако к этой информации следует относиться критически. Естественно, теоретически это возможно, но тогда мощность излучаемого генератором шума должен составлять величину порядка 10...40 Вт, а выходная мощность передатчика «закладки» не должна превышать 20 мВт (при широкополосной частотной модуляции) или 10 мВт (при узкополосной частотной модуляции). Конечно, если речь не идет о приемниках сигналов дистанционного включения в управляемых радиозакладках, которые бесспорно подавляются, а значит, пропадает возможность в нужный момент активировать подслушку. Кстати, надежно блокируются и радиоуправляемые взрывные устройства.

В качестве примера генератора шума можно привести трехканальное устройство ЛГШ-220 (рис. 2.4.49), которое также может быть сделано и в домашних условиях.

Обычно стоимость представленных на рынке генераторов заводского производства колеблется от 250 до 3000 $.

Рассмотрим основные типы таких приборов (рис. 2.4.50).

**Bawler 01** — генератор шума.

**Основные технические характеристики**

Диапазон рабочих частот..... 20...1000 МГц
Выходная мощность..... 1,5...2,5 Вт
Потребляемый ток (при 12 В), не более..... 0,3 А
Напряжение питания..... 9В
Питание..... 220 В, 50 Гц; 12 В

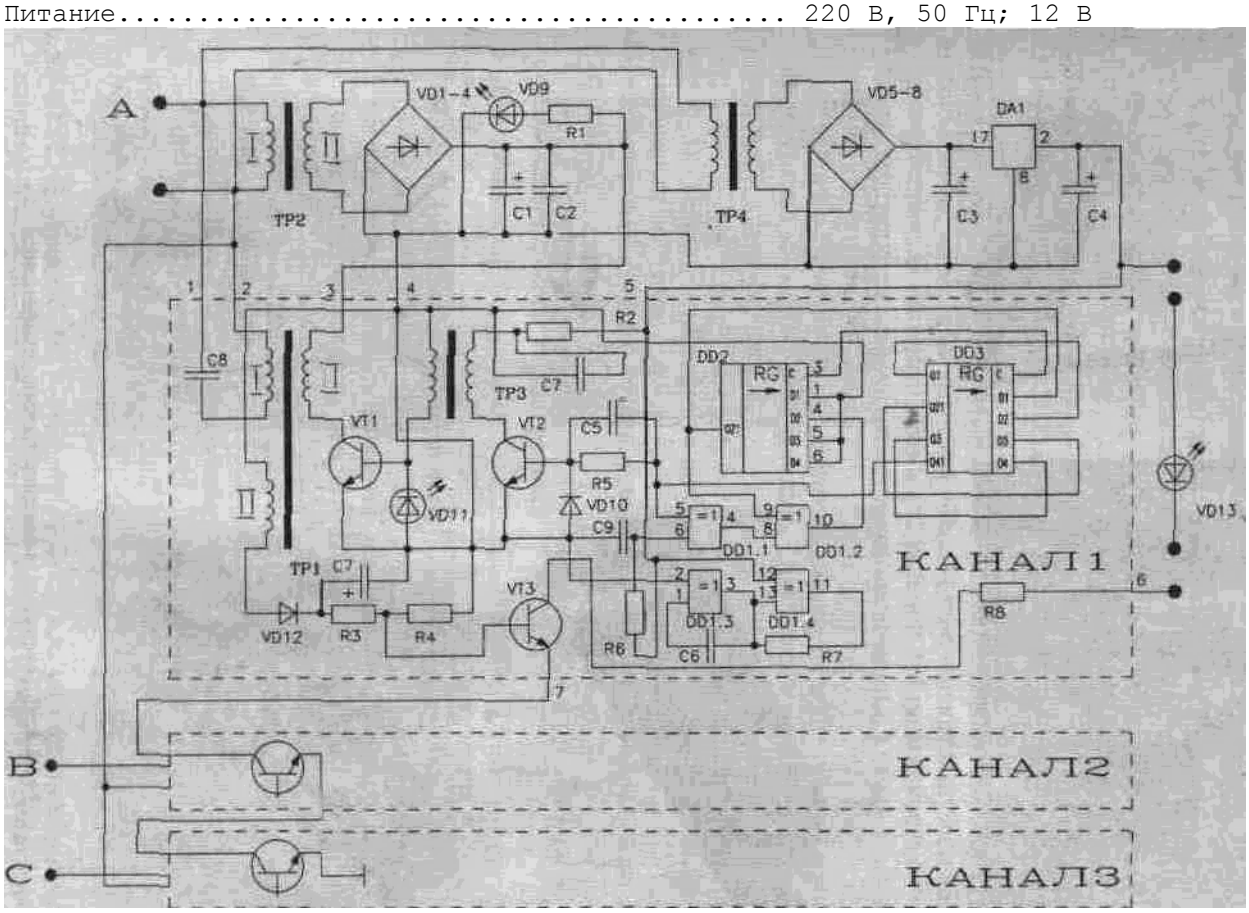



**Рис. 2.4.49. Принципиальная схема трехканального генератора шума ЛГШ-220**

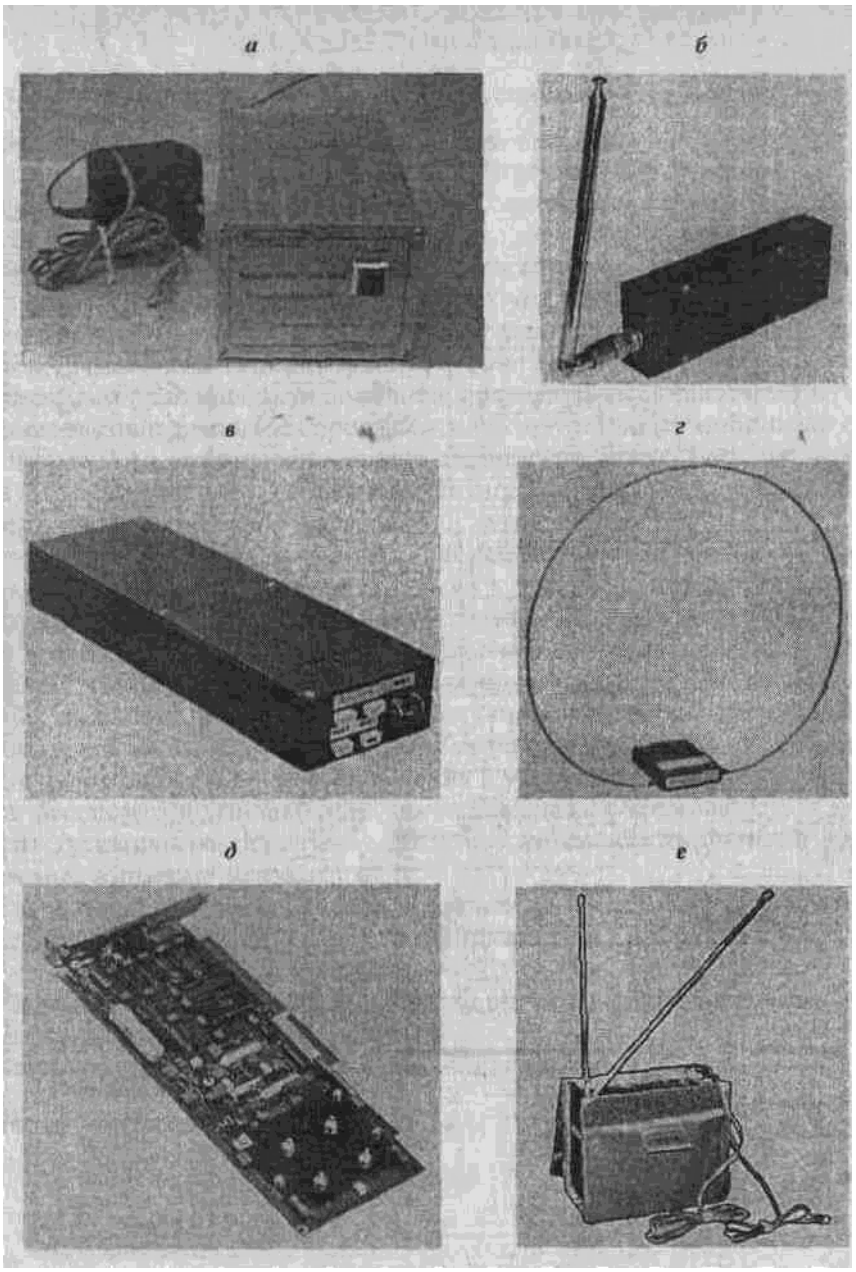



**Рис.2.4.50. Генераторы пространственного зашумления:**
а — Radioveil; б — SP-21B («Баррикада-1»); в — «Гном-3»; г — ПИ-1000; д — «Смог»; е — УАЗИ

**Radioveil** — генератор шума.

**Основные технические характеристики**

Полоса шумовой помехи (-10 дБ) ..... 30...1000 МГц
- Средняя спектральная мощность..... 9 мВт/1 МГц
Мощность выходного сигнала ..... 9 Вт
Потребляемый ток ..... 1 А
Напряжение питания..... 24...36 В
Габариты ..... 170x110x80 мм

**SP-21B («Баррикада-1»)** — портативный генератор радиошума. Отличительной особенностью является обеспечение «белого» шума и наличие телескопической антенны, что в сопряжении с портативностью генератора определяет возможность его использования в любых условиях, в том числе

и в автомобилях.
Генератор обеспечивает гарантированное подавление в радиусе приблизительно 5 м вокруг телескопической антенны (по полусфере) сигналов следующих типов:
>• излучений радиомикрофонов любого типа с модуляцией WFM и мощностью до 50 мВт;
**>•** сигналов ДУ на включение передатчиков радиомикрофонов любого типа.

**Основные технические характеристики**

Диапазон частот..... 5МГц...1ГГц
Антенна..... телескопическая
Уровень сигнала на выходе, не менее..... 45 дБ
Условия эксплуатации температура окружающей среды.....0...40°С
относительная влажность при +25 °С, не более..... 85%
атмосферное давление ..... 750 ±40 мм рт. ст.
Питание..... 12 В
Ток потребления от источника постоянного тока, не более..... 350 мА
Габариты ..... 165х65х25 мм
Масса, не более ..... 0,3 кг

**SEL SP-21B2 «Баррикада-2»** — портативный генератор радиошума. По своим массогабаритным характеристикам аналогичен **«Баррикаде-1».** Генератор обеспечивает:
>• защиту от подслушивающих устройств с радиоканалом мощностью до 20 мВт;
>• подавление приемников сигналов ДУ по радиоканалу в радиусе не менее 30 м.

**Основные технические характеристики**

Диапазон зашумления от телескопических антенн..... 30...1000 МГц
от стационарной антенны ..... 100 кГц...80 МГц
Интегральное значение выходной мощности
при телескопических антенн по выходу 1/2 ..... 9...12 Вт/15...20 Вт
при стационарной антенне .....4 Вт
Потребляемая мощность, не более..... 160 Вт
Питание ..... 220 В, 50 Гц; 12 В, 10 А
Габариты ..... 330х220х190мм
Масса, не более..... 5 кг

**«Гном-3»** — стационарный генератор шума.

**Основные технические характеристики**

Диапазон частот шумового сигнала..... 10 кГц...1 ГГц
Антенны..... рамочные, монтируемые в 3-х плоскостях
Уровень шумового сигнала на выходных разъемах генератора в диапазонах частот:
10... 150 кГц (при полосе пропускания приемника 200 Гц), не менее..... 70 дБ
150 кГц... 30 МГц (при полосе пропускания приемника 90 кГц), не менее..... 70 дБ
30...400 МГц (при полосе пропускания приемника 120 кГц), не менее ..... 75 дБ
0,4... 1 ГГц (при полосе пропускания приемника 120 кГц), не менее..... 70 дБ
Питание ..... 220 В, 50 Гц

**ПП-1000** — стационарный генератор шума. Обеспечивает маскировку побочных электромагнитных излучений устройств вычислительной техники, размещенных на площади 40 кв. м. Устройство имеет индикацию контроля работоспособности, оборудовано разъемом для подключения внешнего контрольного или управляющего устройства, позволяющего автоматически блокировать работу периферийных систем вычислительной техники в случае

возникновения неполадок в работе генератора.

**Основные технические характеристики**

Диапазон частот..... 0,1...1000 МГц
Включение..... вместе с появлением ПЭВМ
Потребляемая мощность ..... 5 Вт
Спектральная мощность шума на расстоянии 1 м в диапазоне, МГц
0,1...100, не менее..... 60 дБ
100...300, не менее..... 70 дБ
300...500, не менее..... 45 дБ
500...1000, не менее ..... 25 дБ
Питание..... от шины компьютера

«Смог» — генератор шума. Бескорпусной генератор шума, устанавливаемый в свободный слот системного блока ПЭВМ. Предназначен для создания активной защиты информации в вычислительных машинах типа IBM PC/AT286, 386, 486 и периферийного оборудования. Сокращает размер контролируемой зоны до нескольких метров.

Программное обеспечение генератора шума функционирует в средах MS DOS, Windows и обеспечивает:

**>•** контроль наличия устройства защиты в ПЭВМ;
>• контроль исправности устройства защиты и антенной системы;
>• прерывание обработки информации в ПЭВМ при неисправности устройства защиты и антенной системы;
>• возможность включения/выключения генератора с клавиатуры ПЭВМ.

Основные технические характеристики

Диапазон частот..... 1 кГц... 1000 МГц
Питание..... от ПЭВМ
Интерфейс с ПЭВМ ..... ISA
Антенные системы..... рамочная — в виде подставки под дисплей и принтер;
дипольная — в виде одиночного провода, закрепляемого вдоль шнура системного блока

**УАЗИ —** устройство активной защиты информации. Предназначено для активной защиты информации от перехвата средствами радиоэлектронного контроля. Работает на две телескопические излучающие антенны, а при необходимости закрытия диапазона частот 100 кГц... 80 МГц рекомендуется дооборудовать помещения дополнительными рамочными антеннами из изолированного провода, проложенного по периметру стен. Для подключения антенн в изделии предусмотрен специальный выход.

**Основные технические характеристики**

Диапазон частот ..... 0...1000 МГц
Интегральное значение выходной мощности
выход 1-й..... 9...15 Вт
выход 2-й..... 15...20 Вт
Мощность в полосе 50...200 кГц на частотах 150 МГц (выход 1) и 450 МГц (выход 2), не менее..... 40 мВт
Полоса частот, соответствующая максимальной выходной мощности
выход 1-й..... 80...300 МГц
выход 2-й..... 400...500 МГц
Спектральная плотность мощности в указанной полосе, не менее.....-38 дБ/Гц
Относительное ослабление выходной мощности в диапазонах частот 0,1...80 и 500...850 МГц, не более..... 36 дБ
Питание ..... 220 В, 50 Гц; 12 В
Потребляемая мощность, не более..... 160 Вт

**«Шатер-К»** —генератор шума.

**Основные технические характеристики**

Выходная мощность сигнала в излучателе, не менее..... 3 мВт
Излучаемые уровни поля..... не превышают норм ГОСТ 121006-84
Диапазон частот, не менее .....0,5... 1000 МГц
Неравномерность спектральной характеристики выходного сигнала, не более ..... 30 дБ на октаву в рабочем диапазоне частот
Питание..... 220 ±22 В, (50 ±2) Гц
Потребляемая мощность, не более..... 35 Вт
Габариты, не более блок питания.....255x190x120 мм
генератор ..... 220x60x40 мм
излучатель ..... 1800мм
Масса изделия с упаковкой, не более ..... 20 кг
Изделие ШАТЕР-К обеспечивает постоянный контроль работоспособности генераторов и блока питания с выдачей сигнализации во внешнюю цепь.
При монтаже генераторов шума, работающих в НЧ-диапазоне (до 30 МГц) особую сложность вызывает размещение многометровых антенн в различных плоскостях.
Для контроля эффективности зашумления целесообразно проверять уровень помехового сигнала в заданном частотном диапазоне и сравнивать его с уровнями ПЭМИ и излучений микроватных специальных технических средств негласного съема информации. Для этого удобно использовать анализаторы спектра.

**Технические средства линейного зашумления**

Выше было отмечено, что технические средства линейного зашумления условно можно разбить на две группы:
>• средства создания маскирующих помех в коммуникационных сетях (телефонных, сигнализации и т. д.);
>• средства создания маскирующих помех в сетях электропитания.

**Средства создания маскирующих помех в коммуникационных сетях**

Принцип их действия основан на генерации в линию шумоподобных сигналов, созданных аналоговым или цифровым способом. Они могут выступать как самостоятельными средствами защиты, так и составной частью более сложных универсальных средств подобных описанным в п. 2.4.3.
**«Туман-1»** — односторонний маскиратор телефонных сообщений. Обеспечивает защиту конфиденциальной информации, принимаемой от корреспондента по телефону на городских и местных (внутренних) линиях. Метод защиты передаваемой информации основан на зашумлении речевого диапазона частот на основе использования псевдослучайной последовательности (ПСП) в тракте соединения абонентов. Выделение полезного сигнала осуществляется абонентом, имеющим маскиратор, путем компенсации созданной им ПСП. Прибор сертифицирован Гостехкомиссией России (сертификат № 187).
Принцип работы с устройством заключается в следующем:
Абонент № 1, имеющий односторонний маскиратор, получает входной звонок от некоего абонента № 2, не имеющего в общем случае такого маскиратора (в том числе таксофон, сотовый телефон). В момент передачи важных сообщений, требующих защиты (о чем абонент № 2 извещает открытым текстом), абонент № 1 подключает к линии маскиратор речи, создающий достаточно интенсивный шум. Этот шум слышит абонент № 2, но продолжает разговор, не меняя голоса. В отличие от него абонент № 1 шума не слышит, он воспринимает «чистую» речь, так как шум при приеме автоматически компенсируется.
К сожалению, маскиратор осуществляет защиту только речи абонента № 2, а телефонная связь ведется в симплексном режиме.

**Основные технические характеристики**

Создаваемое соотношение сигнал/шум
в линии..... —30дБ
Напряжение парафазного ПСП маскирующего сигнала, не менее ..... 15 В

Ток синфазного ПСП-сигнала в телефонной линии, не менее..... 5 мА
Величина остаточного постоянного напряжения в телефонной линии при разговорном режиме, не более ..... 0,6 В
Питание..... 220 В, 50 Гц
Потребляемая мощность, не более..... 15 Вт
Габариты ..... 68х176х170 мм

**NG-301** —устройство защиты телефонных переговоров от прослушивания. Предназначено для защиты телефонных переговоров от прослушивания с помощью средств негласного съема информации. В основе работы NG-301 лежит принцип подачи в телефонную линию шумового маскирующего сигнала. Устройство обеспечивает эффективное противодействие следующим средствам негласного съема информации:

>• радиозакладкам, включаемым в телефонную линию последовательно и параллельно;

>• индукционным датчикам, устанавливаемым на один провод телефонной линии;

>• аппаратуре магнитной записи, подключаемой к телефонной линии с помощью контактных или индукционных датчиков;

>• ТА, факсам, модемам, негласно подключаемым к телефонной линии.

**Основные технические характеристики**

Тип воздействия ..... зашумление
Отношение сигнал/шум в устройстве прослушивания, не хуже..... -20 дБ
Отношение сигнал/шум в ТА, не менее..... 14 дБ
Питание..... 220 В, 50 Гц
Габариты ..... 160х60х220 мм

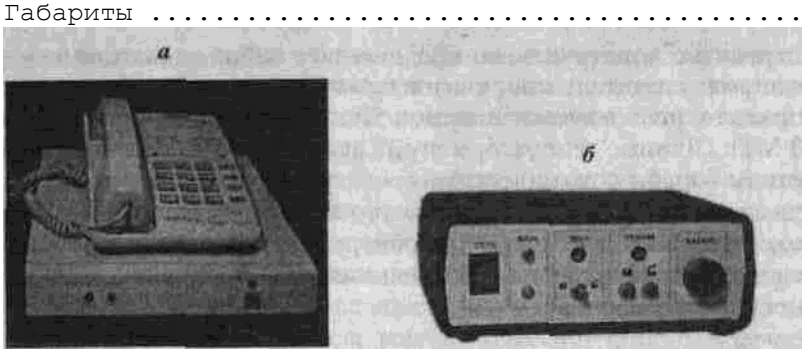



**Рис. 2.4.51. Средства создания маскирующих помех в коммуникационных сетях:**
а — «Туман»; б — «Соната-03»

**SEL SP-17/T** — генератор шума для стандартных телефонных линий. Обеспечивает защиту стандартной телефонной линии пользователя (до АТС) от прослушивания с использованием телефонных передатчиков любого типа и мощности независимо от способа их подключения, средств магнитной записи и параллельных ТА. Принцип действия — создание помех в виде низкочастотного цифровым способом образованного шума с широким спектром.

Генератор не требует подстройки, а также специальных навыков в установке и эксплуатации.

**«Соната-03»** — прибор защиты телефонной линии. Обеспечивает подавление закладных устройств, непосредственно подключаемых к телефонной линии путем постановки активных помех.

**Основные технические характеристики**

Относительное значение уровня маскирующей помеха к уровню полезного сигнала, не менее ..... 35...40 дБ
Питание.....220 В, 50 Гц
Время непрерывной работы, не менее..... 20 ч

Габариты моноблока ..... 115x55x50 мм
Внешний вид некоторых приборов указанного типа приведен на рис. 2.4.51.

**Средства создания маскирующих помех в сетях электропитания**

Для защиты электросетей переменного тока 220 В, 50 Гц от их несанкционированного использования для передачи перехваченной с помощью специальных технических средств речевой информации используются сетевые генераторы шума.

Устройство конструктивно представляет собой задающий генератор «белого» шума, усилитель мощности и блок согласования выхода с сетью 220 В. Как правило, используется диапазон 50... 500 кГц, но иногда он расширяется и до 10 МГц. Данные генераторы шума действительно являются эффективным средством борьбы с техническими средствами негласного съема информации, правда стоят от 200 до 400 $. В некоторых случаях используется более сложная комбинированная аппаратура обнаружения/подавления (генератор включается в режим подавления при превышении ВЧ-сигнала в электросети выше установленного порога).

**NG-201** — генератор шума сетевой. Имеет встроенную систему самодиагностики со световой и звуковой сигнализацией нарушения работоспособности. Обеспечивает высокую эффективность защиты, не требуя при этом специальной подготовки пользователей.

**Основные технические характеристики**

Полоса сигнала защиты .....30...800 кГц
Интегральная мощность сигнала..... 2 Вт
Питание..... 220 В, 50 Гц
Габариты ..... 220x110x50 мм

**NG-401** — генератор шума сетевой. Принцип действия основан на подаче в защищаемую сеть сложного шумоподобного сигнала с цифровым формированием. Модификация изделия NG-402 позволяет защищать одновременно три фазы силовой линии.

**Основные технические характеристики**

Гарантированная полоса частот сигнала защиты .... 80...500 кГц
Мощность сигнала защиты ..... 5 Вт
Питание..... 220 В
Габариты ..... 205x60x155 мм

**NG-402** — генератор шума сетевой. Свипирующий генератор «белого» шума предназначен для защиты электросетей переменного тока 220 В, 50 Гц от несанкционированного их использования для передачи речевой информации. Принцип действия основан на подаче в защищаемую сеть сложного шумоподобного сигнала с цифровым формированием.

**Основные технические характеристики**

Гарантированная полоса частот сигнала защиты .... 80...500 кГц
Мощность сигнала зашиты ..... 5 Вт
Питание..... 220 В
Габариты ..... 205x60x155 мм

**«Соперник»** — генератор шума сетевой. Предназначен для обнаружения и подавления (в автоматическом режиме) устройств несанкционированного съема информации, использующих для передачи данных сеть 220В.

Прибор предназначен для постоянной работы в дежурном режиме. «СОПЕРНИК» постоянно сканирует сеть и анализирует ее параметры. При появлении в ней ВЧ-составляющей загорается красная светодиодная линейка, показывающая уровень сигнала, который присутствует в сети, и сразу же загорается зеленая светодиодная линейка, показывающая уровень шумового сигнала, генерируемого прибором в качестве противодействия. При значении ВЧ-сигнала ниже определенного уровня прибор автоматически переходит в ждущий режим.

**Основные технические характеристики**

Полоса контролируемых частот ..... 30 кГц...1,2 МГц

Порог регистрации сигнала ..... 0,7 В
Максимальная плотность шума генерируемой помехи ..... 0,15 Вт/10 кГц
Ширина спектра шума (на уровне -3 дБ) ..... 5 кГц...1,5 МГц
Индикация принимаемого шума — линейная по амплитуде..... 0,2 В/деление
Индикация генерируемого шума — линейная по мощности..... 0,3 Вт/деление
Мощность шума..... 6 Вт
Потребляемая мощность ..... 10Вт
Габариты ..... 37х63х118 мм
Порог срабатывания прибора выбран таким образом, чтобы не происходило срабатывания на паразитные наводки.

**SP-41C** — генератор шума сетевой.

**Основные технические характеристики**

Амплитуда помехи
в диапазоне 50...500 кГц, не менее..... 10 В
в диапазоне 0,5...5 МГц, не менее..... 1 В
Мощность помехового сигнала ..... 5 Вт
Питание..... 220 В
Вес..... 71,2 кг
Габариты ..... 155х125х40 мм

«Соната-С1» — генератор шума сетевой.

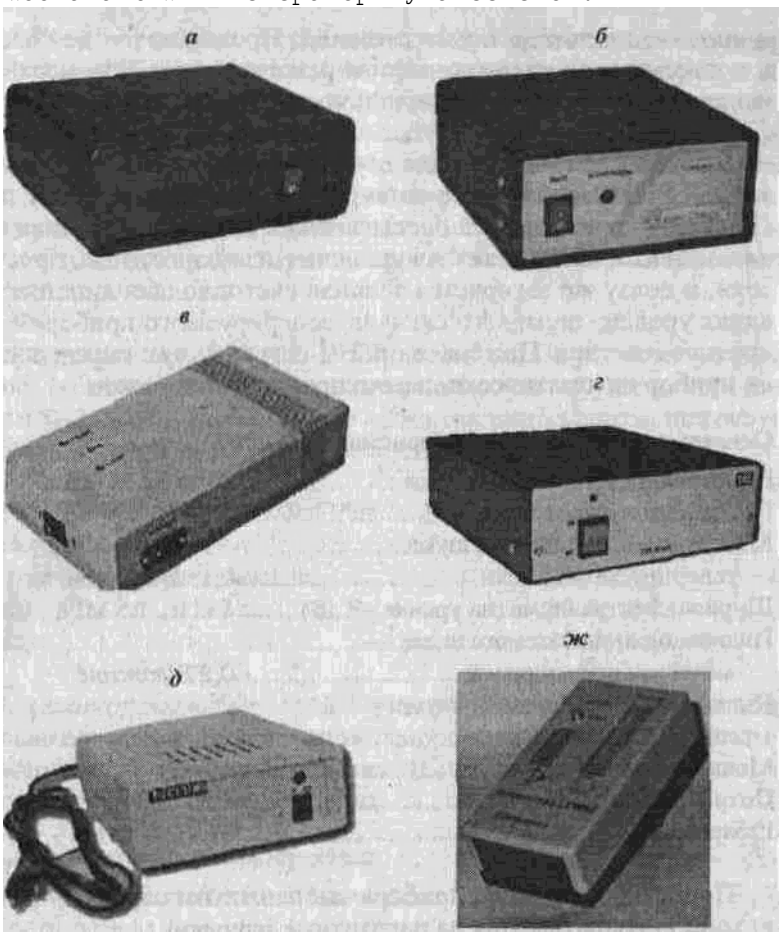



**Рис. 2.4.52. Устройства линейного зашумления электросетей:**
а — «Цикада-С»; б — "Соната-С1"; в — N0-201; г — SP-41C; д — SP-41C; ж — «Соперник»

Основные технические характеристики
Время выхода изделия в рабочий режим

после включения, не более ..... 1 с.
Минимальное сопротивление нагрузки..... 4 Ом
Действующее значение напряжения помехи на нагрузке, не менее.... 10 В
Диапазон частот помехи ..... 0,01...3 МГц
Питание..... 220 В, 50 Гц
Продолжительность непрерывной работы ..... 24 ч
Габариты ..... 153x135x65 мм

**«Цикада-С»**—устройство информационной защиты электросети. Формируемый изделием широкополосный маскирующий сигнал гарантированно защищает электросеть в диапазоне частот 80 кГц... 10 МГц на удалении до 300 м по длине проводки.

**Основные технические характеристики**

Выходная мощность..... 5 Вт
Питание..... 220 В, 50 Гц
Масса ..... 1 кг
Габариты ..... 160x140x60 мм

Изделие не создает помех ПЭВМ и другим устройствам бытовой - электроники.

**«Цикада-СЗ»** — устройство информационной защиты электросети. Соответствует техническим характеристикам изделия «Цикада-С» с дополнительным обеспечением подачи маскирующего сигнала в трехфазную электросеть, организованную по схеме «звезда».

Масса ..... 1,8 кг
Габариты ..... 170x176x68 мм

В большинстве случаев монтаж сетевых генераторов шума не является сложной проблемой — достаточно включить прибор в сеть и в некоторых случаях провести несложные регулировки. Однако в ряде помещений могут использоваться несколько вводов по питанию (подключение от разных фаз розеток и освещения, специальное стабилизированное питание для ПЭВМ и т. д.), и тогда необходимо защищать их все. Внешний вид некоторых устройств линейного зашумления электросетей показан на рис. 2.4.52.

**Многофункциональные средства защиты**

При практической организации действительно надежной защиты помещения от утечки информации по техническим каналам необходимо комплексное использование различных устройств безопасности: акустических, виброакустических, сетевых генераторов шума и источников электромагнитного маскирующего излучения. При этом можно решить задачу следующими тремя путями:

>• подбором различных устройств защиты и их автономным использованием;
>• объединением различных устройств защиты в единый комплекс путем применения универсального блока управления и индикации;
>• использованием готовых комплектов промышленного производства.

Рассмотрим особенности каждого из этих путей.

В первом случае при привлечении к выбору состава и типа приборов квалифицированного специалиста возможен подбор оптимального по техническим, эргономическим и стоимостным параметрам комплекта аппаратуры. Однако практическое применение его потребует от пользователя последовательного включения всех источников шума и индивидуального контроля их работоспособности, что не всегда удобно.

Во втором случае используется готовый пульт управления, устраняющий описанный выше недостаток, например «Соната-ДУ».

**«Соната-ДУ»** — блок дистанционного управления комплексом создания маскирующих помех.

Он предназначен для дистанционного скрытного включения/выключения комплекса технических средств защиты информации, имеющих сетевое электропитание.

**Основные технические характеристики**

Максимальная мощность коммутируемой нагрузки..... 100 Вт
Вид канала управления ..... радиоканал, ИК-канал
Питание ..... 220 В, 50 Гц
Продолжительность непрерывной работы изделия ..... до 24 ч
Габариты основного блока..... 135x65x155 мм
Примечание. Благодаря наличию встроенной системы самопрограммирования для управления устройством может быть использован любой пульт ДУ от бытовых устройств (телевизоров, кондиционеров) или практически любой брелок включения автосигнализации.
Однако не всегда аппаратуру разных фирм-производителей Возможно включать с помощью одного универсального пульта.
Рассмотрим третий путь — использование готовых многофункциональных комплектов на следующих примерах.
**«ГРОМ-ЗИ-4»** — многофункциональный генератор шума. Предназначен для защиты информации от утечки за счет побочных электромагнитных излучений (ПЭМИ) от средств оргтехники, а также для создания помехи устройствам несанкционированного съема информации в телефонных линиях и электрических сетях. Выполнение всех указанных функций обеспечивается данным генератором независимо друг от друга.
При защите телефонных переговоров от подслушивания генератор «размывает» спектр акустических сигналов в телефонной линии. Работа генератора при зашумлении радиодиапазона осуществляется на съемную телескопическую антенну. При зашумлении крупногабаритных объектов (вычислительных центров, терминальных залов и т. п.) целесообразно использование нескольких комплектов **«Гром-ЗИ-4»** с антеннами, ориентированными в трех взаимно перпендикулярных плоскостях.
**Основные технические характеристики**
Полоса частот помехового сигнала при зашумлении радиодиапазонов ..... 20...1000 МГц
Типовое значение напряженности поля помех, создаваемого генератором, относительно 1 мкВ/м в диапазоне 20...60 МГц..... 60 дБ
60...300 МГц .....90 дБ
300...1000 Мгц .....40 дБ
Полоса частот, занимаемая помеховым сигналом при зашумлении электросети ..... 100... 1000 кГц
Напряжение помехового сигнала в электросети, относительно 1 кВ, не менее..... 60 дБ
Напряжение помехового сигнала, создаваемого в телефонной линии на частоте 20 Гц..... 2,5 В
в полосе частот 15...25 кГц..... 0,5 В
Время непрерывной работы..... 8 ч
**«Гром-ЗИ-6»** — генератор шума. Предназначен для защиты переговоров от утечки информации по телефонной линии и электрической сети. Прибор защищает участок линии от ТА до АТС, а также блокирует устройства, использующие электрическую сеть помещения в качестве канала утечки информации.
Принцип действия прибора основан на маскировке спектра речи широкополосным шумом. Прибор предотвращает прослушивание ТА устройствами, работающими по принципу ВЧ-навязывания, а также реагирующими на поднятие трубки ТА.
Генератор может работать в автоматическом и неавтоматическом режимах. В автоматическом режиме контролирует напряжение линии и включает защиту при поднятии трубки ТА и снижении напряжения линии в случае подключения к ней параллельного телефона или подслушивающего устройства. Прибор имеет сертификат Гостехкомиссии при Президенте РФ.
**Основные технические характеристики**
Максимальное значение напряжения, генерируемого прибором по телефонной

линии, в диапазоне частот 6...40 кГц, не менее..... 3 В
Отношение напряжения помех, генерируемых прибором в линию, к напряжению помех на клеммах ТА, не менее.....30 дБ
Диапазон регулировки тока линии, не менее ..... 10 мА
Напряжение помех, генерируемых прибором в электросеть относительно 1мкВ в диапазоне частот
0,1... 1 МГц, не менее ..... 60 дБ
1...5 МГц, не менее..... 30 дБ
Время непрерывной работы..... 8 ч
Генераторы «Гром-ЗИ-4» и «Гром-ЗИ-6» стоят весьма дорого, но не имеют всех необходимых для полноты защиты функций (например, не могут создавать виброакустического шума), и их приходится дополнять аппаратурой других типов.
Существуют и другие универсальные комплексы. В качестве примера рассмотрим систему комплексной защиты «Скит».
**«СКИТ»** — многофункциональный комплекс защиты. Он обеспечивает защиту:
>• от утечки информации за счет ПЭМИН (в соответствии с требованиями Гостехкомиссии России);
>• от утечки информации по виброакустическому каналу.
Кроме того, осуществляет обнаружение и подавление до трех одновременно работающих специальных технических средств разведки с передачей перехваченной информации по радиоканалам. Комплекс управляется по ИК-каналу при помощи пульта ДУ.
В состав комплекса входят:
«Скит-СК» — автоматический высокоскоростной коррелятор-подавитель радиомикрофонов;
«Скит-УМ» — усилитель мощности генератора прицельной помехи;
«Скит-Ш» — широкополосный генератор электромагнитных помех;
«Скит-Т» — широкополосный генератор помех для телефонных и слаботочных линий;
«Скит-С» — широкополосный генератор помех для силовой сети электропитания;
«Скит-ВА» — генератор виброакустических помех речевого диапазона частот с комплектом датчиков (8 штук);
«Скит-К» — дистанционно-управляемый коммутатор средств защиты;
камуфлированный ИК-приемник сигналов ДУ.


**Рис. 2.4.53. Многофункциональные средства защиты:**
а — «Соната-ДУ»; б — «Гром-ЗИ-6»

Независимо от типа применяемых систем линейного и пространственного зашумления порядок работы с ними должен быть следующим:
>• определяются возможные технические каналы утечки информации;
>• устанавливается степень их опасности и потенциальная возможность перехвата информации;
>• определяются требования к аппаратуре защиты (типы и количество генераторов шума и датчиков, возможность их сопряжения и т. д.);
>• разрабатывается технический проект объекта в защищенном исполнении;
>• осуществляется монтаж закупленного оборудования;

>• проводится комплексный технический контроль эффективности принятых мер;
**>•** проводится периодический контроль работоспособности аппаратуры.
Внешний вид некоторых типов многофункциональных систем защиты представлены на рис. 2.4.53.

**2.4.7. Защита информации от высокочастотного навязывания**

При рассмотрении методов ведения промышленного шпионажа в п. 1.3.5. были выделены основные принципы применения методов ВЧ-навязывания для съема информации с различных объектов. Теперь остановимся на методах защиты в соответствии с вышеизложенным материалом по каждому из возможных каналов воздействия.

**Защита от ВЧ-навязывания в проводных каналах**

Защита информации от высокочастотного ВЧ-навязывания в проводных каналах осуществляется с помощью как организационных, так и технических мероприятий.
К организационным мероприятиям относятся:
>• использование ТА, выполненных в защищенном виде;
>• осуществление физического контроля телефонных линий на предмет наличия подключений на расстояниях до 100 м от аппарата (расстояние выбрано исходя из предельной дальности действия систем перехвата информации такого типа);
>• отключение ТА от сети на время проведения переговоров.
Однако организовать постоянный контроль телефонных линий в реальных городских условиях достаточно проблематично. Это можно сделать только при размещении организации в обособленном здании либо при наличии собственной АТС. Отключение аппаратов от линии на время проведения переговоров также нельзя отнести к надежным мероприятиям — опыт показывает, что об этом часто забывают. Поэтому по-настоящему надежной защиты не может быть без применения технических средств и проведения технических мероприятий.
Технические мероприятия проводятся по следующим направлениям:
>• инструментальный контроль излучений проводов на предмет выявления зондирующих ВЧ-сигналов в линиях связи;
>• установка пассивных схем защиты.
Рассмотрим перечисленные технические способы более подробно. Проведение технического контроля телефонных линий на предмет выявления зондирующих сигналов — технически легко осуществимое мероприятие. Для этого необходимо иметь приемник со следующими характеристиками:
>• частотный диапазон 9 кГц... 30 МГц;
>• чувствительность порядка нескольких единиц микровольт;
>• наличие АМ- и ЧМ-детекторов.
Кроме того, требуется обеспечить прием сигналов, распространяющихся по проводным линиям. Для этого можно использовать обычные электрические и магнитные антенны, например электрические типа HE 010, HE 013/015, HFH 2Z1 и магнитные HFH 2-Z3, HFH 2-Z2. Могут использоваться упоминавшиеся ранее комбинированные антенны, предназначенные для измерения как магнитной, так и электрической составляющей поля, например FMA-11 или LA-320 (рис. 2.4.54). Однако располагать антенны следует в непосредственной близости от проводов телефонной сети. Очень эффективны для этих целей специальные антенны типа токосъемных клещей.
Радиоприемная аппаратура, которая может использоваться для обнаружения подобных излучений, была подробно описана в п. 2.3. Кроме того, в табл. 2.4.4 приведены технические характеристики приемных устройств, наи-

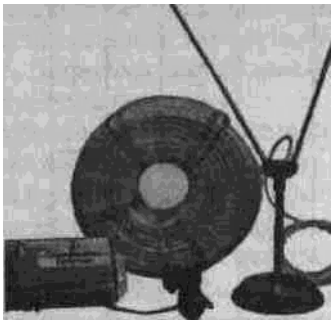


**Рис. 2.4.54. Комбинированная антенна LA-320**

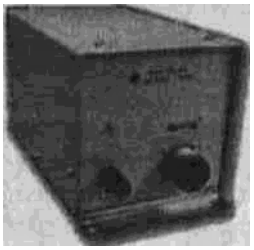


**Рис. 2.4.55. Фильтр сетевой ФСП-1Ф-7А**

более полно удовлетворяющих требованиям контроля именно в проводных каналах связи.

Недостатком рассматриваемого метода защиты является возможность выключения аппаратуры перехвата информации во время проверки, следовательно, эпизодический контроль оказывается не вполне надежным. «Доброжелатели» вполне могут пожаловать между проверками.

Гарантированным способом противодействия является шунтирование линии или микрофона телефонной трубки конденсатором емкостью порядка 0,01 мкФ. Он имеет предельно низкую цену, но обеспечивает достаточно надежную защиту. Зондирующий сигнал по законам физики идет «по пути наименьшего сопротивления», а конденсатор для высокой частоты имеет относительно низкое по сравнению с микрофоном сопротивление.

В связи с этим обстоятельством интересен тот факт, что как у нас, так и за границей существуют предприниматели, которые весьма успешно продают «защищенные от ВЧ-навязывания телефонные аппараты» по цене до нескольких сотен долларов. Экономическая нецелесообразность приобретения подобной техники очевидна.

Для защиты от прослушивания помещений с помощью ВЧ-навязывания по сетям 220 В, например путем воздействия на различные радиотехнические приборы или электрический звонок, хорошие результаты можно получить при использовании специальных сетевых фильтров типа **ФСП-1Ф-7А** (рис. 2.4.55), **ФПС-3Ф-10А.**

**Защита информации от ВЧ-навязывания в радиодиапазоне**

Основная сложность применения пассивных и полуактивных радиозакладных устройств, описанных в подразделе 1.3.1, — это необходимость проникновения на объект с целью их установки, что требует проведения специальных

**Таблица 2.4.4. Приемные устройства для обнаружения ВЧ-излучений в проводных каналах**

Модель /Диапазон, МГц /Вид модуляции /Чувствительность, мкВ (с/ш=12дБ) /Шаг настройки, кГц /Количество каналов памяти /Габариты, мм /Вес, кг

IC-R72 /0,03...30 /AM, FM, SSB, CW /0,5...1 /0,01; 0,1; 1; 5; 9; 10;1000 /99 /241x94x229 /5,5

IC-R71A/E /0.1...30 /AM, FM, WFM, SSB, FSK, CW /0.3...3 /0,01; 1; 1000 /32 /286x110x276 /7,5

HF150 /0,03...30 /AM, FM, SSB /0,2...2 /1 /- /185x80x175 /1,3

AR 3030 /0,03...30 /AM, FM, WFM, USB, LSB, CW /0,3...30 /0,005; 0,01; 1; 1000 /- /250x88x240 /2,2

FRG-100 /0.005...30 /AM, FM, SSB, CW /0.25...10 /0,001; 0,1; 1 /- /238x93x243 /3

TS-140 /0,15,..30 /AM, FM, SSB, CW /0.25...10 /- /- /270x96x270 /6,1

STV-301 /0,01...30 /AM, FM, WFM /2 /- /- /360x320x130 /7

FSM 11 /0,01...30 /AM, FM, WFM /0,1 /0,2; 1,7; 9 /- /450x145x545 /26

операций. В качестве примера в том же подразделе был приведен исторический случай проведения мероприятия по внедрению «орла» в американское посольство. Вернемся к нему еще раз, чтобы четко сформулировать требования по обеспечению защиты.

Так, перед непосредственными исполнителями была поставлена задача получения достоверной информации из американского посольства в Москве. Агентурное проникновение было весьма затруднено, подходов к американским дипломатам практически не имелось. Поэтому рассматривались различные варианты мероприятий, которые смогли бы обеспечить конспиративность постановки спецтехники и съема информации. Обычные классические методы внедрения технических средств для организации контроля разговоров были неприемлемы, т. к. не было соответствующей агентуры для внесения в помещения каких-либо предметов-камуфляжей, в которых располагалась бы техника для съема информации. К тому же было известно, что американская служба безопасности постоянно осуществляет в своем посольстве в Москве контроль эфира в диапазоне радиоволн, на которых имеется возможность работать передатчиками обычных радиозакладок для съема информационных сигналов.

В связи с этим начались исследования по созданию различных вариантов новой спецаппаратуры съема информации с использованием нетрадиционных принципов создания технических устройств. В результате остановились на методе облучения высокой частоты нелинейного, пассивного эндовибратора (микрофона).

Помимо разработки принципиально нового вида спецтехники было уделено серьезное внимание созданию камуфляжа для обеспечения максимума безопасности. Было решено смонтировать спецтехнику внутри овального предмета из алебастра и гипса с рельефной символикой в виде американского национального герба. А сама пористость поверхности герба была достаточна для прохождения звуковых колебаний, вызванных энергией человеческого голоса к микрофону.

Контрольный пункт для приема информативных сигналов от «герба» разместился в помещениях гостиницы «Националь» (речь идет о старом здании Посольства США в Москве, располагавшемся на Манежной площади).

Следующим этапом в проведении мероприятий по получению информации из кабинета американского посла стала разработка убедительной легенды для внесения «герба» в здание посольства. В день национального праздника Америки в посольство пришла пионерская делегация и в торжественной обстановке вручила американскому послу «герб». Посол поблагодарил за приятный подарок и повесил «герб» у себя в кабинете на стене, над письменным столом.

Однако в случае более четких действий службы безопасности появление подобного подарка в кабинете, где обсуждаются конфиденциальные вопросы, было бы невозможно. Сотрудники спецслужб полностью понадеялись на проверку «орла», поскольку по существующему порядку все вносимые предметы (особенно в такую ответственную зону, как кабинет посла) подвергались тщательному обследованию, в том числе рентгеновскому просвечиванию, которые ничего не дали. Действительно, выявить подобные

устройства крайне сложно и самый действенный метод защиты — никаких подарков не принимать.
Второй недостаток данной системы, который возможно использовать для организации защиты, — это очень большие уровни мощности передатчика. Современные приборы легко обнаруживают такое излучение. Трудность заключается только в том, что необходимо зарегистрировать излучение непосредственно в момент перехвата информации. Кроме того, такая интенсивность сигнала опасна для здоровья как поднадзорного лица, так и самого злоумышленника.
Кабинет американского посла многократно проверялся стандартными методами на наличие радиозакладок с отрицательным результатом. Однако американская спецслужба решилась серьезно заняться поиском техники съема информации, которая, как они предполагали, установлена в здании посольства в Москве. Поэтому из США прибыли специалисты с соответствующей аппаратурой. События происходили следующим образом: была проведена рутинная проверка, после чего специалисты удалились. Шторы на окнах оставались открытыми, и наблюдатели зафиксировали, что посол приступил к диктовке писем секретарю. Сотрудники с аппаратурой в это время ползали под подоконником с радиоприемным устройством и скрытно разворачивали антенны. Вот тут и было обнаружено направленное излучение высокой частоты. После этого определили место. Вначале со стены был снят «герб», а саму кирпичную стену почти всю разобрали. Образовалось большое отверстие с выходом на улицу. «Герб» несколько дней лежал в кабинете, и только затем они решили посмотреть, нет ли чего-нибудь у него внутри. «Герб» разломали и нашли резонатор.
Следовательно, для обнаружения факта облучения необходимо проводить либо постоянный радиоконтроль, либо провоцировать противостоящую сторону на применение средства разведки в известные сроки. Обнаружение зондирующего ВЧ-сигнала — довольно простое дело даже для неспециалиста. Для этих целей необходим панорамный радиоприемник или анализатор спектра, например из числа описанных в подразделе 2.3.3. Выбранный прибор переводится в режим максимального обзора при минимальной чувствительности, и осуществляется изучение радиоэлектронной обстановки в районе расположения объекта (идентифицируются все мощные излучения). Антенны поворачиваются в сторону возможного расположения передатчиков. После этого достаточно фиксировать появление зондирующих сигналов. Главная сложность — периодические ложные срабатывания: включаются радиотелефоны в прилегающих помещениях, радиомаяки различного назначения, мощные радиостанции армии и спецслужб, которые работают не постоянно.
Еще один способ защиты — экранирование помещения. Способ действенный, но проблема состоит только в том, что он очень дорогой и резко снижающий эргономические характеристики помещения. Особую сложность вызывает защита окон и дверей. Другое направление — размещение помещений, выделенных для проведения особо конфиденциальных мероприятий, в заглубленных железобетонных подвалах.

**Защита информации от ВЧ-навязывания в оптическом диапазоне**

Для обеспечения защиты от лазерных микрофонов возможно использование организационных и технических мероприятий. Последние, в свою очередь, реализуются путем различных видов воздействия на канал перехвата информации активными и пассивными средствами в оптическом и акустическом диапазонах.
**К организационным методам** можно отнести:
**>•** использование погодных и климатических условий (дождь, снег, сильный ветер и т. д.);
>• ведение переговоров в местах с высоким уровнем фоновых шумов (как внешних, так и внутренних), например в ресторане;

>• размещение на местности таким образом, чтобы на пути распространения лазерного луча были естественные и искусственные препятствия (кустарник, строения и т. д.);
>• использование недоступных для лазерного подслушивания помещений (окна выходят во двор; подвальные, полуподвальные помещения);
>• расположение рабочих мест, исключающих прохождение акустических сигналов к окнам;
>• использование аппаратуры предупреждения о применении лазерных систем;
>• ведение беседы без повышения голоса, не срываясь на крик (разница в уровне речи между нормальным и громким голосом может достигать 15 дБ);
>• максимальное увеличение расстояния до границы контролируемой территории;
>• увеличение расстояния от говорящего до окна.

К применению организационных мероприятий необходимо подходить разумно. Например, глупо было бы специально ждать резкого ухудшения погоды, чтобы провести конфиденциальную беседу.

Более надежными являются **технические методы** защиты информации. Так, радикальным средством защиты в оптическом диапазоне является прерывание сигнала с использованием ставней, экранов и т. д. Однако это приводит к отсутствию в помещении дневного света. Представляется возможным ослабить зондирующий лазерный сигнал и путем его рассеивания, поглощения или отражения. Технической реализацией данных способов является использование различных пленок, наносимых на поверхность стекла. Таковы в общих чертах возможности противодействия пассивными методами в оптическом диапазоне.

При использовании методов активного противодействия задача сводится к электромагнитному воздействию на приемные (а возможно, и передающие) тракты аппаратуры разведки с целью выведения их из строя либо временного ухудшения работоспособности.

Целью противодействия в акустическом диапазоне является уменьшение отношения сигнал/шум в точке ведения съема (на поверхности стекла), при которых восстановление речевой информации невозможно (-10...-14 дБ). Решить данную задачу можно двумя способами:
>• увеличением уровня маскирующего шума, т. е. применением активных средств акустической маскировки;
>• снижением уровня сигнала, т. е. усилением звукоизоляции окна.

В настоящее время существует большое количество типов систем активного зашумления в акустическом диапазоне. Они используются для подавления дистанционных и забрасываемых средств перехвата речевой информации. В существующих системах формируется маскирующий сигнал типа «белый» шум или типа «разговор трех и более лиц», спектр которого представляет собой усредненный спектр голоса человека. Однако у подобных систем имеется целый ряд недостатков.

**Во-первых**, значительно повышается уровень фоновых акустических шумов в защищенном помещении, что приводит к быстрой утомляемости находящихся в нем людей.

**Во-вторых**, при разговоре в зашумленном помещении человек инстинктивно начинает говорить громче, тем самым повышается величина отношения сигнал/помеха на входе приемника, акустической разведки. Таким образом, с учетом того, что активная акустическая маскировка ухудшает эргономические показатели, основным путем защиты речевой информации является обеспечение необходимых акустических характеристик ограждающих конструкций выделенных помещений.

Звукоизолирующая способность ограждающих конструкций определяется отношением величины интенсивности J1 прошедшего через ограждение звука, к интенсивности падающего J2, и характеризуется коэффициентом:

t=J1/J2.
В расчетах и измерениях наиболее часто используют величину, называемую звукоизоляцией или потерями на прохождение звука через препятствие (ограждение) и определяемую соотношением
R=101g(1/t).
Значение звукоизоляции для различных типов ограждающих конструкций и нескольких акустических частот приведены в табл. 2.4.5. Необходимо отметить, что существенное влияние на звукоизоляцию оконных конструкций оказывает наличие в них щелей и отверстий.
Наиболее совершенными в настоящее время являются конструкции окон с повышенным звукопоглощением на основе стеклопакетов с герметизацией воздушного промежутка и с заполнением промежутка между стеклами различными газовыми смесями. Стеклопакеты устанавливаются в выполненных из различных металлов переплетах. Стекла выбираются разной толщины и устанавливаются с небольшими наклонами относительно друг друга. Все это позволяет при значительном ослаблении сигнала избежать резонансных явлений в воздушных промежутках. В результате интенсивность речевого сигнала на внешнем стекле оказывается значительно ниже интенсивности фоновых акустических шумов и съем информации традиционными для акустической разведки методами оказывается невозможным.
Наиболее радикальной мерой защиты является прерывание канала распространения звука. Это достижимо только в случае применения вакуумной звукоизоляции. В основе способа лежит физическое явление, состоящее в том, что звук не может распространяться в пустоте. Таким образом, теоретически при вакууме

**Таблица 2.4.5. Звукоизолирующие свойства некоторых типов ограждающих конструкций**

Тип конструкции /Акустическая частота, Гц
/500 /1000 /2000 /4000
Кладка в 1/2 кирпича /42 /48 /54 /60
Кладка в 2 кирпича, отштукатуренная /59 /65 /70 /70
Плита железобетонная, 50 см /35 /45 /51 /58
Щитовая дверь /24 /24 /24 /23
Двери тяжелые двойные с облицовкой тамбура /65 /70 /70 /71
Одинарное остекление, 3 мм /22 /28 /31 /32
Двойное остекление, 4мм, между стеклами — 200 мм /39 /47 /54 /56
Тройное комбинированное остекление/71 /66 /73 /77

между точкой ведения разведки и источником речи получается идеальная звукоизоляция. Однако на практике достичь полного прерывания невозможно, так как требуется обеспечить герметизацию не только промежутка между стеклами, но и пространства между переплетом и рамой, а кроме того, предотвратить структурное распространение звука через материал рам.
Окна обычной конструкции имеют довольно низкий уровень звукоизоляции (см. табл. 2.4.5). Кроме того, на степень звукоизоляции влияют:
>• герметичность швов между стеклом и переплетом, переплетом и оконной рамой, оконной рамой и стеной;
>• длина, высота и размер поперечного сечения переплета и стекла;
>• поглощение звука в звукопоглощающих элементах между стеклами и рамой;
>• особенности конструкции и способы ее изготовления и т. д.
Широкое распространение получили и так называемые акустические экраны, которые используются при невозможности применения стационарных методов звукоизоляции. Обычно применяются передвижные, складные и легко

монтируемые акустические экраны.
С целью решения задач по защите помещений акустические экраны могут быть использованы, например, для дополнительной защиты окон, имеющих низкую звукоизолирующую способность.
В целом можно утверждать, что применение даже простейших приемов позволит избежать перехвата информации либо существенно ухудшит качество записи перехваченного разговора.
Таким образом, организация защиты информации от перехвата лазерными микрофонами возможна самыми разнообразными способами и средствами. Поэтому необходимо провести оптимизацию существующих мер защиты при их комплексном использовании, так как наличие большого количества противоречивых требований и ограничений (в основном эргономических и стоимостных) требует проведения многосторонней оценки эффективности системы защиты объекта от лазерных систем перехвата речи.

**Защита информации от ВЧ-навязывания вирусов**

Как указано в подразделе 1.3.5, дистанционное внедрение компьютерных вирусов с помощью ВЧ-навязывания в настоящее время не является актуальной угрозой, но в недалеком будущем сможет наносить существенный урон государственным и коммерческим структурам. В связи с этим рассмотрим возможные способы защиты информации, циркулирующей в ЭВМ, реализация которых возможна с помощью организационных, программных и технических мер.

**К организационным мерам** можно отнести следующие:

>• увеличение радиуса контролируемой территории вокруг объекта электронно-вычислительной техники (это ведет к необходимости существенно увеличивать мощность передатчика ВЧ-навязывания);

>• обучение персонала по обнаружению признаков воздействия ВЧ-сигналов (помехи на экране монитора, сбои в работе отдельных устройств и т. д.);

>• осуществление контроля доступа к линиям связи, терминалам, сетям электропитания и другим элементам сети и вспомогательного оборудования;

>• расположение электронно-вычислительной техники в заглубленных помещениях, бетонных зданиях и использование естественных экранов на пути возможного распространения ВЧ-сигналов.

**Программные меры** — подразумевают использование систем антивирусной защиты и будут рассмотрены в разделе 2.6.

К дополнительным **техническим мерам** следует отнести:

>• создание и использование системы предупреждения о применении «вирусного орудия» путем проведения постоянного радиоконтроля на предмет выявления мощных электромагнитных сигналов вблизи ЭВМ;

>• экранирование персонального компьютера, соединительных кабелей, другого оборудования или в целом зданий и сооружений;

>• установка фильтров в цепях электроснабжения, управления и связи;

>• широкое внедрение оптоволоконных соединений.

Таким образом, угрозе информационной безопасности при использовании ВЧ-навязывания можно противопоставить известные и относительно недорогие средства защиты.

## 2.5. Защита от несанкционированной аудиозаписи

### 2.5.1. Обнаружители диктофонов

В разделе 1.5 отмечалось, что диктофон может быть использован как в качестве закладного подслушивающего устройства, так и для негласной записи доверительных бесед какой-либо из заинтересованных сторон. В одном случае его тайно устанавливают в контролируемом помещении и

только периодически меняют кассеты, в другом — прячут в личных вещах или под одеждой.

Данный прибор прост и надежен и в силу этого обстоятельства пользуется большой популярностью, но, к сожалению, не только у честных бизнесменов, которые без всяких черных намерений любят на досуге проанализировать ход переговоров, но и у промышленных шпионов, и у разного толка провокаторов. Поэтому задача защиты от несанкционированной аудиозаписи является достаточно актуальной. Существуют два основных направления ее решения:

- это предотвращение проноса звукозаписывающих устройств в контролируемые помещения;
- фиксация факта применения диктофона и принятие адекватных мер.

Первый способ может быть реализован только при наличии достаточно мощной службы безопасности и весьма солидных финансовых средств. Так, в соответствии с применяемыми в устройствах обнаружения физическими принципами можно выделить следующие виды аппаратуры, способные решать эти задачи:

- металлодетекторы;
- нелинейные радиолокаторы;
- устройства рентгеноскопии;
- специальные детекторы диктофонов.

Металлодетекторы могут применяться на входах в помещение или при наружном досмотре лиц и носимых ими предметов (кейсов, сумок и т. п.). Эти приборы бывают двух видов: стационарные и переносные. Переносные портативные приборы достаточно подробно описаны в подразделе 2.3. Стационарные арочные металлообнаружители (рис. 2.5.1), как правило, имеют следующие основные характеристики:

- высота — 2000 мм;
- ширина — 800 мм;
- глубина — 500 мм;
- скорость прохода — до 1 м/с;
- питание от сети однофазного тока напряжением 220 В.

Существенным недостатком арочных конструкций является высокая сложность камуфлирования аппаратуры под предметы интерьера, поскольку спрятать его можно только в достаточно узком дверном проеме или арке. От этого недостатка в значительной степени избавлены панельные стационарные металлодетекторы. Примером такого прибора может служить **«Панель»**. Конструктивно он выполнен в виде двух плоских панелей, образующих контролируемый проход, и выносного блока сигнализации и управления. Такая конструкция дает возможность легко закамуфлировать прибор под интерьер офиса.

Металлодетектор «Панель» имеет следующие характеристики:

- высота — 1400 мм;
- ширина — 600 мм;

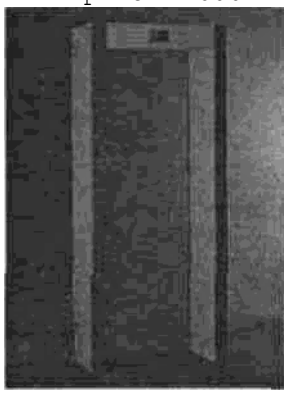


**Рис. 2.5.1. Стационарный арочный металлодетектор**

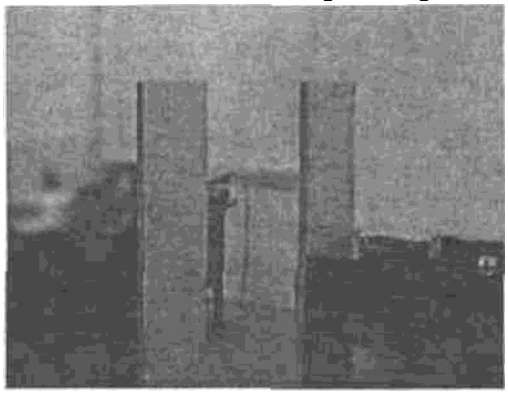


**Рис. 2.5 2. Металлодетектор «Панель»**

>• глубина — 40 мм;
>• масса панелей — 15 кг;
>• питание — однофазное напряжением 220 В;
>• потребляемая мощность — 30 Вт.

Вследствие ограниченной чувствительности металлодетекторов надежность обнаружения таких мелких объектов, как современные микрокассетные диктофоны, в большинстве случаев оказывается недостаточной, особенно когда нежелательно или просто невозможно проведение открытого досмотра. Таким образом, металлодетекторы можно рассматривать только как вспомогательное средство в комплексе с другими, более эффективными мероприятиями по обнаружению и подавлению средств звукозаписи. На рис. 2.5.3 приведена примерная схема организации поста контроля для ведения проверки в негласном режиме.

На постах такого типа аппаратура контроля камуфлируется под предметы интерьера. Главной трудностью является обеспечить строго заданный маршрут движения посетителей. Тип ручной клади при контролируемом человеке тоже должен быть ограничен визиткой, дамской сумочкой, папкой для бумаг и т.д. В качестве дополнения к стационарному металлодетектору часто используются портативные металлоискатели, скрытно размещенные в кейсах или на теле персонала поста контроля.

В этом случае наиболее целесообразно использовать малогабаритные металлодетекторы типа **«Сфинкс ВМ-311».** Прибор имеет следующие характеристики:

**>•** габариты 190х75х32 мм;
**>•** вес — 200 г;
>• питается — от 9-вольтовой батарейки типа «Крона».

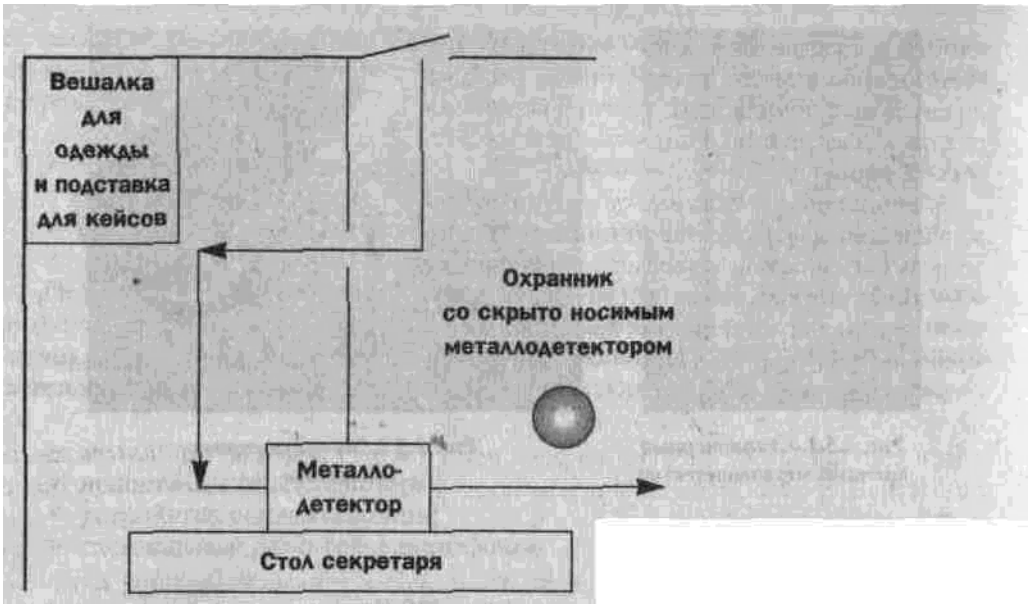



**Рис. 2.5.3. Схема поста скрытого контроля**

Устройство легко прячется в рукаве пиджака и не привлечет внимание посетителя, даже если будет случайно перед ним «засвечено», поскольку имеет совершенно безобидный внешний вид (рис. 2.5.4). Однако, несмотря на скромные размеры, при грамотном использовании оно позволяет обнаружить небольшую монету с расстояния в 6 см, а нож — с 13 см. Индикация — световая и звуковая.

Нелинейные радиолокаторы способны обнаруживать диктофоны на значительно больших расстояниях, чем металлодетекторы, и в принципе могут использоваться для контроля за проносом устройств звукозаписи на входах в помещения. Однако при этом возникают такие проблемы, как уровень безопасного излучения, идентификация отклика, наличие «мертвых» зон, совместимость с окружающими системами и электронной техникой.

В настоящее время наиболее полное практическое решение проблем обнаружения скрытно проносимых диктофонов методом нелинейной локации обеспечивает система **G-1400.** Имеется также модификация данной системы **(G-1500),** которая размещается в боковых панелях стандартного арочного металлодетектора.

Системы **G-1400 и G-1500** легко обнаруживают даже одиночный точечный диод в створе между передающей и приемной антеннами шириной 130 см. При этом энергетическая СВЧ-нагрузка в 2000 раз меньше предельной безопасной нормы, допускаемой согласно ГОСТ 12.1.006-84, то есть совершенно безвредна как для обследуемых лиц, так и для персонала службы безопасности. Конфигурация и состав системы обеспечивают сплошную ВЧ-завесу по всей площади поперечного сечения прохода. Требуемая эффективность и надежность

**Рис. 2.5.4. Портативный металлодетектор «Сфинкс ВМ-311»**

работы достигаются за счет совместного использования с

металлодетектором, а также в результате обучающего тестирования оператора и настройкой с полным учетом местных условий.
Устройства рентгеноскопии позволяют надежно выявить наличие диктофонов, но только в проносимых предметах. Очевидно, что область применения этих средств контроля крайне ограничена, так как они практически не могут использоваться для целей личного досмотра и скрытого контроля. Вместе с тем аппаратура такого типа производится серийно, и достаточно широко используется при таможенном досмотре. Например, стационарный рентгеноскоп **«Шмель-ТВС»** имеет следующие характеристики:
>• максимальные габаритные размеры просматриваемой ручной клади — 500x700x400 мм;
>• запоминание — более 1000 изображений;
>• время получения изображения — 2с;
>• питание — от сети однофазного тока напряжением 220 В;
>• потребляемая мощность — 1500 Вт.
Блок управления имеет возможность подключения внешнего компьютера, что позволяет при необходимости проводить дополнительную обработку изображений, распечатать их на принтере, обеспечить голосовое сопровождение при записи.

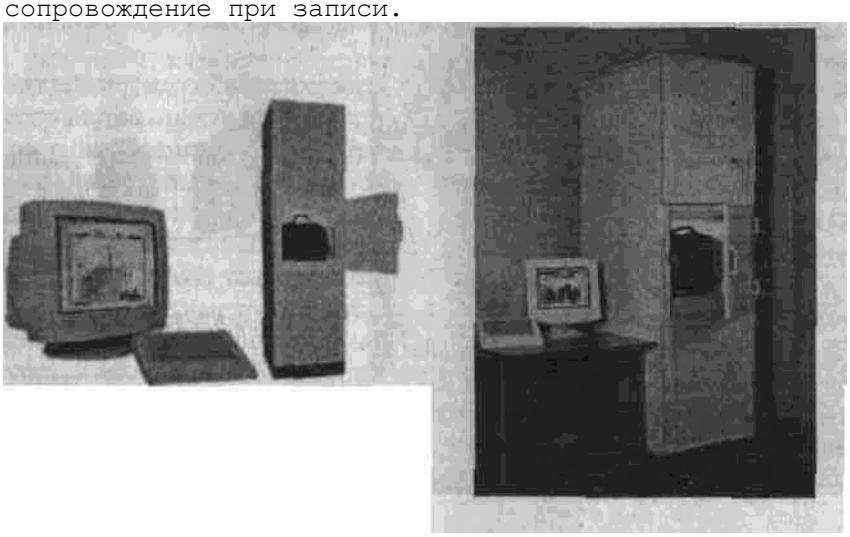


**Рис. 2.5.5. Аппаратура рентгеновского контроля «Шмель-ТВС»**
Помимо стационарной аппаратуры имеются и мобильные приборы. Например, комплекс **«Шмель 90-К»** предназначен для проведения экспресс осмотра в масштабе реального времени, а также для поиска устройств съема информации в предметах интерьера. Он универсален, мобилен и очень прост в эксплуатации. Состоит из небольшого рентгеновского аппарата, совмещенного с автономным источником питания, и легкого визуально-анализирующего устройства, фиксируемого в различных положениях на подставке. Внешний вид комплекса представлен на рис. 2.5.6.
Аппаратура имеет следующие технические характеристики:
>• рабочее поле контроля — круг диаметром 255 мм;
>• вес рентгеновского аппарата — 6,5 кг;
>• вес визуально-анализирующего устройства — 2,9 кг.
Необходимость и возможность практического использования рентгеновской аппаратуры следует рассматривать комплексно, в контексте конкретных задач и существующих местных условий. Вместе с тем стоит отметить, что вопреки расхожему мнению современные образцы рентгеновской техники создают минимальные дозовые нагрузки на обследуемый объект, не влияющие даже на кинофотоматериалы. Для лучших образцов этой техники доза — менее 100 микрорентген за одно обследование. Вместе с тем помня «Чернобыльский синдром», все-таки необходимо считаться с устоявшимися

понятиями и предрассудками при принятии того или иного решения.

Специальные устройства для определения наличия работающих диктофонов.

**Рис. 2.5.6. Переносной комплекс «Шмель 90-К»**

Различают два принципа работы таких устройств, основанных на эффекте обнаружения акустических сигналов и выявлении побочных электромагнитных излучений (ПЭМИ).

Характерный шум лентопротяжного механизма и щелчки при нажатии на кнопки — обычные явления для кассетных магнитофонов 70-80-х годов. Поэтому для маскировки их работы применяли специальные приемы, от помещения приборов рядом с источниками звука (типа часов) до перебора во время беседы четок, чтобы замаскировать стуком костяшек щелчки диктофона. Однако эти времена канули в Лету, поскольку у подавляющего количества современных приборов выявить акустический сигнал от лентопротяжного механизма при обычном фоне в помещении и других помех практически невозможно. А цифровые диктофоны — вообще абсолютно бесшумны (п. 1.3.4).

Таким образом, регистрация побочных электромагнитных излучений сейчас является единственно» возможным способом выявления работающих диктофонов.

Как правило, работа многих обнаружителей диктофонов (особенно портативных) основана на принципе выявления излучений от генератора стирания — подмагничивания (ГСП). Однако при работе таких обнаружителей возникают следующие проблемы:

>• используемый частотный диапазон характеризуется большим количеством источников мощных магнитных полей (телевизоры, контактная сеть городского транспорта, лампы дневного света, электродвигатели бытовых приборов и т. д.), которые буквально «глушат» излучения диктофонов гораздо эффективнее, чем во времена оные глушили «забугорные» радиостанции;

>• многие из современных диктофонов иностранного производства вообще не имеют ГСП. Стирание обеспечивается постоянным магнитом, а подмагничивание — так называемой «постоянной составляющей».

Следовательно, для обнаружения самых современных средств звукозаписи данные устройства практически непригодны.

Теоретически возможно осуществить обнаружение побочных излучений, возникающих в результате самовозбуждения электронного устройства из-за паразитных связей в генераторных и усилительных каскадах, например микрофонного усилителя. Однако измерения показывают, что дальность возможной регистрации ПЭМИ такого рода (в диапазоне 20 кГц... 50 Мгц)

не превышает нескольких сантиметров для бытовых средств звукозаписи, а от специальных устройств с металлическим корпусом вообще не регистрируются даже высокочувствительными лабораторными приборами.
Существуют устройства, которые реагируют на переменное магнитное поле, возникающее при работе электродвигателей. В лаборатории они работают очень четко, но на практике главной трудностью их реализации является наличие большого числа источников низкочастотных магнитных полей, разнообразие спектральных портретов излучений диктофонов разных типов, низкие уровни сигналов. Правда, металлические корпуса диктофонов уже не являются препятствием для обнаружения полей данного типа.
В результате анализа этой «информации для размышления» можно сделать вывод об объективной сложности создания по-настоящему надежной аппаратуры выявления работающей звукозаписывающей техники. И тем не менее попытки создать подобные устройства не прекращаются, а ряд моделей даже имеется в продаже.
В общем виде данная аппаратура включает в себя следующие блоки:
**>•** низкочастотную магнитную антенну, выполненную конструктивно как отдельный элемент и выносимую как можно ближе к предполагаемому месторасположению диктофона;
**>•** детекторный блок, выполняющий операцию обнаружения ПЭМИ, с регулируемым порогом срабатывания;
**>•** фильтры, ограничивающие полосу частот, в которых осуществляется контроль; иногда добавляют и режекторные (то есть «закрывающие» определенные диапазоны) фильтры, настроенные на частоты наиболее мощных источников местных помех (как правило, они конструктивно выполнены в детекторном блоке);
>• устройства световой (шкала светодиодов, стрелочный индикатор, контрольная лампочка) и звуковой (вибрационной) индикации наличия ПЭМИ (конструктивно выполняются или в детекторном блоке, или выносятся на специальный пульт);
>• блок питания.
Рассмотрим некоторые примеры практической реализации данных средств. На первый взгляд, наилучший вариант представляет собой изделие РК 645-SS, реализующее первое направление борьбы с диктофонами. Плоские магнитные антенны размещаются по периметру двери. Дальность обнаружения стандартного звукозаписывающего прибора — до 1 м. Однако существенный недостаток — полная невозможность обнаружения выключенных диктофонов, то есть если человек входит в кабинет (здание) с неработающим диктофоном, а только затем его включает, то система его не зафиксирует. Следовательно, такое устройство необходимо дополнять другими: арочным металлоискателем и нелинейным локатором, а это уже очень и очень дорогое удовольствие.
Интересной отечественной разработкой является обнаружитель диктофонов **PTRD-018** (Portable tape recorder detector). Он предназначен для скрытного обнаружения работающих магнитных звукозаписывающих устройств. Прибор состоит из блока регистрации и 4 (8 или 16) датчиков, которые устанавливаются стационарно (например, в стол, за которым ведутся наиболее важные

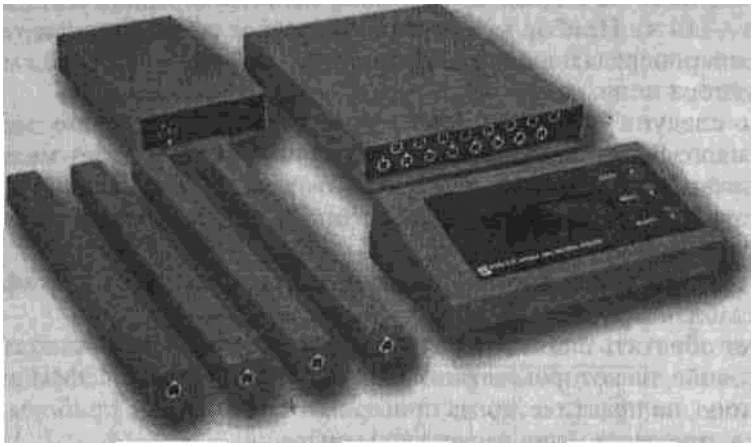


**Рис. 2.5.7. Устройство обнаружения диктофонов PTRD-018 (вариант с 4-мя датчиками)**

переговоры, или в подлокотники кресла клиента). Внешний вид комплекса приведен на рис. 2.5.7.

Используемым признаком, по которому обнаруживается диктофон, служит электромагнитное поле, создаваемое работающим электродвигателем лентопротяжного механизма. Отметим, что спектр этого электромагнитного поля лежит в диапазоне очень низких частот, и вследствие этого даже металлические корпуса «фирменных» приборов для скрытой звукозаписи не защищают их от обнаружения данным устройством.

Основным препятствием к обнаружению сигнала устройствами подобного типа является электромагнитное поле промышленных помех как на основных частотах, так и на их гармониках (вплоть до 9-й), что существенно ограничивает применение таких приборов. Кроме того, выявление факта применения цифровых диктофонов оказывается принципиально невозможным.

Существуют и портативные варианты обнаружителей работающих диктофонов, которыми можно пользоваться и за пределами офиса. В качестве примера может служить изделие **TRD 009V** фирмы CCS. Размеры устройства позволяют легко разместить его в кармане. Сигнал тревоги — легкая вибрация корпуса. При этом, чем вы ближе к диктофону, тем сильнее вибрация. Питание от встроенных аккумуляторов, для удобства

**Рис. 2.5.8. Детектор диктофонов TRD-800**

потребителя имеется индикатор разряда и внешнее зарядное устройство (время заряда — 14 ч). Прибор может использоваться также для обнаружения излучений микропередатчиков в диапазоне 1...1000 МГц, то есть выступать в роли детектора поля.

Однако следует учесть тот факт, что на практике подобные портативные системы малоэффективны, поскольку их применение требует максимального приближения датчика к предполагаемому месту нахождения диктофона. Приходится буквально обнимать собеседника, что не только неудобно, но и

просто нетактично.
Характеристики некоторых обнаружителей работающих диктофонов приведены в табл. 2.5.1.
Следует обратить внимание на тот факт, что в таблице указано максимальное расстояние, на котором датчик может среагировать на ПЭМИ диктофона. К сожалению, на практике, когда применяют специальные приборы для скрытой записи, это расстояние несколько меньше.

**2.5.2. Устройства подавления записи работающих диктофонов**

Из материалов предыдущего подраздела видно, что обнаружение диктофона — очень сложная техническая задача. Вместе с тем работающий на запись диктофон можно подавить, то есть создать условия, при которых запись невозможна. Существуют следующие виды воздействия на диктофоны:
>• на сам носитель информации, то есть на магнитную ленту;
**>•** на микрофоны в акустическом диапазоне;
>• на электронные цепи звукозаписывающего устройства.
Первый способ нашел применение в устройствах типа размагничивающей арки, которая устанавливается в тамбуре входной двери и создает мощное переменное магнитное поле (обычно с частотой сети или ей кратной). В результате находящиеся в тамбуре предметы (в том числе и кассеты с записанной информацией) размагничиваются.
Устройства характеризуются высоким энергопотреблением и опасны для здоровья, особенно тех лиц, которые пользуются различного рода внедренными в организм электронными стимуляторами. Поэтому организация, применяющая такие системы, обязана информировать посетителей о наличие опасности, что является демаскирующим фактором и приводит к тому, что по настоянию клиента разговор может состояться за стенами данного учреждения.
Системы противодействия, использующие принцип воздействия непосредственно на сам микрофон, можно разделить на две группы:

**Таблица 2.5.1. Основные характеристики некоторых типов обнаружителей диктофонов**

Характеристика /PTRD-016 /PTRD-018 /TRD-800 /RM200 /РК 645-S /РК 645-SS
Страна-изготовитель /Россия /Россия /США /Россия /Германия /Германия
Максимальная дальность обнаружения от датчика, м /до 0,7 /до 1,5 /до 0,5 при наличии ГСП /до 0,5 f /ДО 1 /до 1
Количество датчиков /4 /4/8/16 /1 /до 6 /1 /6
Питание, В /220 /220 /— /- /9 /220
Потребляемая мощность, Вт /0,6 /0,8 /- /- /- /-
Габариты, мм / / / / / /
Основного блока /160x110x20 /160x80x40 /22x57x89 /170x170x30 /25x70x25 /Одна 135x130x50 и две 235x130x50
Датчика /170x20x20 /170x20x20 / /230x35x25 / /

>• воздействие на микрофон в ультразвуковом диапазоне с целью перегрузки
микрофонного усилителя;
>• использование генератора активных акустических помех в речевом диапазоне.
Системы ультразвукового подавления излучают мощные неслышимые человеческим ухом ультразвуковые колебания (обычно частота излучения — около 20 кГц), воздействующие непосредственно и на микрофоны диктофонов, и акустические закладки, что является их несомненным достоинством. Данное ультразвуковое воздействие приводит к перегрузке усилителя низкой частоты, стоящего сразу после акустического приемника. Перегрузка усилителя приводит к значительным искажениям записываемых (передаваемых) сигналов, часто до степени, не поддающейся дешифровке.

Например, комплекс **«Завеса»** при использовании двух ультразвуковых излучателей способен обеспечить подавление диктофонов и акустических закладок в помещении объемом 27 м$^3$. Комплекс состоит из генератора, нескольких излучателей, предназначен для работы в замкнутом пространстве и обеспечивает защиту, в зависимости от необходимости, какой-либо локальной области или помещения в целом. Минимальная конфигурация комплекса — двухканальная (два излучателя). При необходимости имеется возможность наращивания до 4-х, 6-ти, 8-ми и т.д. каналов. Как уже говорилось в разделе 2.4, поскольку воздействие осуществляется по каналу восприятия акустического сигнала, то совершенно не важны дальнейшие трансформации, способы и каналы передачи перехваченной информации, так как информационный сигнал подавляется на этапе его восприятия. Последнее соображение особенно ценно именно при противодействии использованию диктофонов, поскольку с целью улучшения качества запись этих приборов особенно часто обрабатывается с помощью специальной аппаратуры. Внешний вид комплекса был приведен на рис. 2.4.47.

Однако системы ультразвукового подавления имеют важный недостаток: эффективность их резко снижается, если микрофон диктофона или «закладки» прикрыть фильтром из специального материала или в усилителе с низкой частотой установить фильтр низких частот с граничной частотой 3,4...4 кГц.

Вторая группа средств подавления, использующая генераторы активных акустических помех в речевом диапазоне, применяется в ограниченных случаях. Действительно, трудно представить себе доверительный разговор между партнерами под аккомпанемент генератора шума мощностью в 75...90 дБ. Примерами таких приборов являются ANG-2000, ANG-007, **NG-502M**, **RNG-01** и т.д. Все эти изделия были достаточно подробно описаны в подразделе 2.4.6.

Впрочем, некоторого внимания заслуживает одна из последних моделей подобной техники — генератор акустического шума **SOUND PRESS**. Данный прибор используется для защиты от несанкционированного съема акустической информации путем маскировки полезного звукового сигнала «белым» шумом корректированного спектра. Изменение спектра проведено таким образом, что позволяет в полной мере воздействовать на микрофоны и входные тракты устройств несанкционированного съема информации при пониженном воздействии на слуховые органы человека и его нервную систему. Прибор имеет следующие технические характеристики:

- мощность шума — 2 Вт;
- полоса равномерной плотности шума — 2—10 кГц;
- срез спектра шума — < 2 кГц;
- размер — две колонки по 80x100x150 мм каждая.

Необходимо отметить, что изделие эффективно в помещениях площадью не более 15—18 кв. м. Если площадь больше, надо покупать еще один комплект или ограничить переговорную зону. При этом колонки должны быть разнесены на максимальное расстояние и направлены на говорящих. Уровень сигнала зашумления устанавливается вручную, исходя из субъективного восприятия дискомфорта, но в любом случае нельзя устанавливать громкость ниже половинной мощности. В рекламном проспекте сказано, что обеспечивается вполне комфортное проведение переговоров. Безусловно, прибор осуществляет прекрасную защиту от всех видов акустических «подслушек», однако понятие комфортности ограничивается тем, что после более-менее длительных переговоров под его аккомпанемент, в отличие от других систем, у участников не болят голова и уши. Впрочем, если слух и нервы в обоих партнеров в молодости хорошо натренированы частым посещением дискотек, то это средство маскировки вполне приемлемо. Ну и, конечно же, ни о каком скрытном применении такого рода аппаратуры не

может быть даже и речи.
Кроме стационарных моделей имеются и миниатюрные приборы для акустического подавления диктофонов в «полевых условиях». Например, акустический генератор белого шума WNG-022 (Рис. 2.5.10). Прибор имеет размеры 98x71x30 мм и питается от батарейки в 9 В.

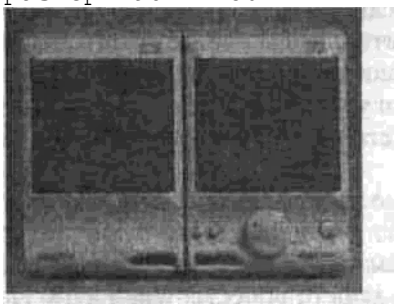


**Рис. 2.5.9. Генератор акустического шума SOUND PRESS**

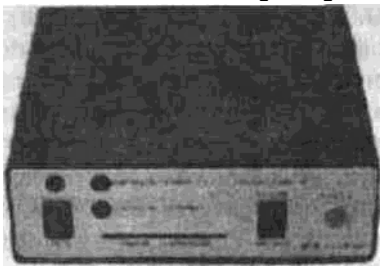


**Рис. 2.5.10. Акустический генератор белого шума WNG-022**

Одновременно мы просто обязаны развеять одно очень распространенное заблуждение. Многие считают, что совершенно не нужно тратиться на специальные генераторы акустического шума. Вполне достаточно просто включить погромче во время переговоров музыку или беседовать в ванной, открыв на полную мощность воду. Тот, кто так думает, жестоко ошибается. Специальная аппаратура легко выделит полезный сигнал из такого рода «шумов». Маскирующая помеха должна быть особым образом подобрана, только тогда она надежно прикроет полезный сигнал.
Поскольку бизнесмены, как правило, все-таки следят за своим здоровьем, то наибольшее распространение получили устройства, где подавление осуществляется способом воздействия на электронные цепи диктофона. Для этих целей используются системы воздействия на электронные цепи диктофона подавления типа **«Рубеж»** (рис. 2.5.5), **«РаМЗес»**, **«Шумотрон»**, **«Буран»**, «УПД».
Принцип действия таких устройств основан на генерации в дециметровом диапазоне волн электромагнитных колебаний, несущая которых модулирована шумоподобным или хаотическим импульсным сигналом.
Излучаемые направленными антеннами помехи, воздействуя на элементы электронной схемы диктофона, вызывают в них шумоподобные наводки. Вследствие этого одновременно с речью осуществляется запись и шума, что приводит к значительному искажению записываемой информации или вообще к полному ее подавлению.
Зона подавления зависит от мощности излучения, а также от типа используемых антенн. Обычно это сектор с углом от 30 до 80 град и радиусом до 1,5 м (для диктофонов в экранированном корпусе). Для диктофонов в пластмассовом корпусе дальность подавления может выроста до 6 и даже больше. Если диктофон оборудован выносным микрофоном, то дальность подавления становится еще больше за счет того, что соединительный кабель выполняет роль антенны, принимающей излучение от аппаратуры подавления.
Еще один момент, на который следует обратить внимание. Если

записывающее устройство находится у его владельца на теле (в костюме и т. д.), то не исключен факт, что речь самого хозяина диктофона необязательно, но может и записаться, а вот с записью речи собеседника наверняка будут большие проблемы. Это произойдет из-за того, что звуковое давление, воздействующее на микрофон записывающего устройства, создаваемое голосом хозяина диктофона и его собеседника, несоизмеримы по уровню. Владельцу подавителя важно как раз то, чтобы не записали именно его речь. Это и происходит благодаря применению системы подавления.

Некоторые типы диктофонов в режиме записи (**UHER**, **DICTAPHONE**, некоторые модели **SONY**, **PANASONIC** и т. д.) при попадании в зону подавления начинают сами «шуметь» в акустическом диапазоне, выдавая тем самым намерения своего хозяина. Так что если у вашего собеседника в кармане вдруг что-то зашумело при включении подавителя диктофонов, значит он хотел вас записать, и принятые меры предосторожности не напрасны.

Интересно отметить, что данная аппаратура будет одинаково успешно «давить» запись как кинематических, так и цифровых диктофонов. Какая ему разница, что «давить»?!

Одним из приборов вышеописанного типа является изделие **«Рубеж-1»** (рис. 2.5.11). Более мощной и современной системой является **«РаМЗес-Дубль».** Основные технические характеристики которого приведены в табл. 2.5.2.

Обычно подобные приборы используются в офисе, но возможно их применение и в автомобилях с питанием от бортовой сети, иногда применяется камуфляж в виде «кейса».

Другим примером может служить подавитель диктофонов **«Шумотрон-2»**, работающий в импульсном режиме на частоте 915 МГц. Длительность излучаемого импульса в приборе — не более 300 мкс, а импульсная мощность — не менее 150 Вт; таким образом, при средней мощности излучения 20 Вт обеспечивается дальность подавления диктофонов в экранированном корпусе (типа Olimpus-400) до 1,5 м в секторе около 30 град. Дальность подавления диктофонов в неэкранированном корпусе составляет несколько метров.

Таблица 2.5.2. Основные технические характеристики изделия «РаМЗес-Дубль»

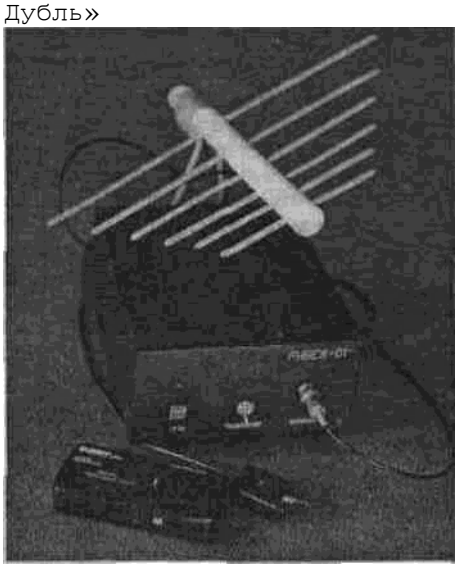


**Рис. 2.5.11 Внешний вид изделия «Рубеж-1»**

Характеристика /Значение

Телесный угол зоны подавления, град /70

Дальность подавления диктофонов (корпус металл/пластмасса), м /1,5/6

Рекомендуемое время непрерывной работы, ч /Не ограничено

Питание, В /220
Габариты, мм: /
блок подавления /245x180x70
антенна /340x220x30
Излучаемая мощность (на одну антенну/на две), Вт /8/2x4
Масса, кг/3

## 2.6. Защита информации в компьютерных сетях

### 2.6.1. Виды потенциально опасных воздействий

Защита информационных ресурсов, хранящихся и обрабатываемых в компьютерных системах, как никогда стала актуальной в связи с широким внедрением последних во все области нашей жизни. Причем возникла парадоксальная ситуация, когда сама информация превратилась в некий вид товара, который можно купить, продать или использовать каким-либо третьим способом, приносящим немалый доход. Стоимость подобного товара зачастую превосходит в десятки и даже сотни раз стоимость вычислительных средств, в рамках которых эта информация функционирует.

Сами компьютеры стали орудием и объектом информационных атак, а само деяние получило свою правовую оценку как уголовное преступление. Статья 272 Уголовного кодекса Российской Федерации предусматривает ответственность за неправомерный доступ к компьютерной информации с максимальным наказанием в виде лишения свободы на срок до 3 лет (см. п. 1.1).

В соответствии с целями различают два вида потенциально опасных воздействий на компьютерные системы: умышленные и неумышленные.

Основными видами умышленного воздействия можно считать:

>• заражение компьютерными вирусами;

>• несанкционированный доступ к информации.

Под результатами целенаправленных потенциально опасных воздействий на компьютерные системы обычно понимают: хищение, копирование и модификацию информации.

Не меньший урон могут нанести и неумышленные воздействия, связанные с ошибками персонала, так как их результатом может стать утрата важных сведений, хранящихся на машинных носителях (рис. 2.6.1).

Ошибки персонала не относятся к преднамеренным воздействиям, однако они могут иметь не менее опасные последствия, поэтому рассмотрение способов защиты начнем именно с них.

### 2.6.2. Защита от ошибок обслуживающего персонала

Компьютер — это сложная самонастраивающаяся система, работающая с минимальным участием оператора. Особенно высокой степени автоматизации внутренних процессов компьютеров корпорации Microsoft удалось достигнуть с введением новой спецификации Plug and Play, которая практически

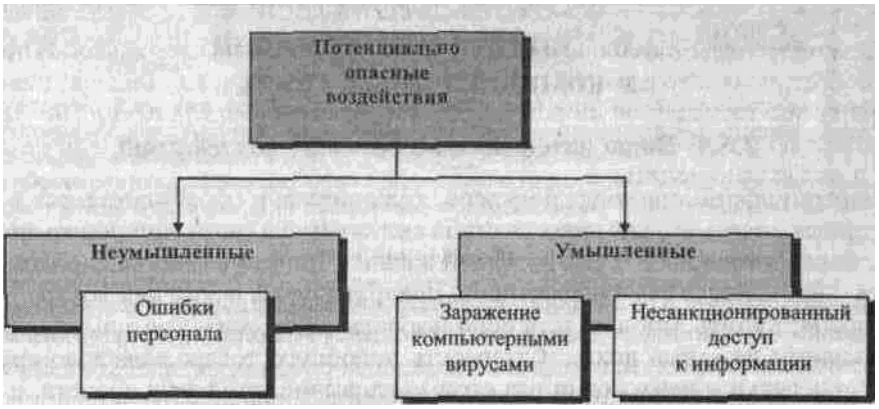



**Рис. 2.6.1. Виды потенциально опасных воздействий на компьютерные системы**

освободила пользователей от проведения многих сложных настроек. При этом вся информация о системе храниться в так называемом реестре.

Реестр (Registry) — это централизованная база данных, которая содержит всю конфигурационную информацию Windows'95(СМ.Сноску 1)(Windows'98) о параметрах настройки системы и приложений.

Линия технической поддержки Microsoft принципиально не отвечает ни на какие вопросы по поводу реестра, так как корпорация официально заявляет, что пользователи не должны никоим образом вносить изменения в реестр по той причине, что эти изменения могут повредить их компьютер.

Поэтому если вы не хотите в один прекрасный день узнать о неработоспособности ваших вычислительных средств, то вам необходимо предупредить своих сотрудников о запрете каких-либо работ с реестром (файлы **Regedit.exe**, **System.dat**, **User.dat**, **System.da0 и User.daO** в каталоге Windows). Так как все вносимые изменения происходят очень быстро (без привычного подтверждения) и могут привести к потере данных, блокировке системы и даже повреждению аппаратных средств.

Однако справедливости ради, надо отметить, что иногда для того, чтобы заставить какое-либо приложение работать или повысить его производительность, нет другого пути, кроме редактирования реестра. Но это можно делать только в исключительных случаях и при соблюдении следующих правил:

**>•** вы точно знаете правильные значения ключей реестра и параметров, а также ограничения для конкретных устройств и приложений;

>• все попытки установить или модифицировать конкретную функциональную возможность с помощью опций Панели управления (Control Panel) не удались;

>• операция выполняется под руководством специалиста.

___

Сноска 1. Здесь и далее вопросы защиты от ошибок рассмотрены на примере операционной системы Windows'95, как получившей в настоящее время наибольшее распространение.

___

Тем не менее, если однажды, включив компьютер, вы неожиданно получите сообщение о невозможности найти файл реестра: Registry File was not found. Registry services may be inoperable for this session (Файл реестра не найден. Сервис реестра недоступен для данного сеанса), то вы должны точно знать, что и как нужно делать.

**Создание резервных копий**

Надо отметить, что создание резервных копий является средством защиты не только от ошибок в реестре, но и от других ошибок и преднамеренных действий, связанных, например, с удалением рабочих пользовательских

файлов, заражением компьютерными вирусами и т. д. Однако ничто не приводит к таким глобальным последствиям, как ошибки в реестре, поэтому поговорим о них более подробно.

Администраторы, отвечающие за безопасность компьютерной информации, знают, что реестр содержит два таких важных файла, как **User.dat и System.dat.** В файле **User.dat** содержится информация, специфичная для конкретных пользователей, например предпочтительная настройка рабочего стола и т. д. В файле **System.dat** хранится информация, характеризующая данную систему, например аппаратные профили и параметры настройки сети.

Оба файла **— User.dat и System.dat** — являются скрытыми и хранятся в каталоге **C:\Windows.** Так как файлы скрытые, то просматривать их лучше с использованием программ-оболочек **Norton-Commander** или **Volkov-Commander.** Для того чтобы получить доступ к скрытым файлам непосредственно из Windows'95, необходимо с помощью меню кнопки «Пуск» (Start) открыть окно «Проводник» (Explorer) Панели задач; в сервисной строке выбрать функцию **Вид** и в раскрывшемся меню — опцию **Параметры.** На появившейся вкладке следует установить флажок на функцию **Отображать все файлы.** После этой операции атрибут **Скрытый** окажется снятым.

При инсталляции Windows'95 система автоматически создает файлы **User.dat** и **System.dat** и резервные копии для каждого из них. Эти резервные копии называются, соответственно, **User.da0 и System.da0** и также представляют собой скрытые файлы в каталоге **C:\Windows.** Резервные копии нужны на тот случай, если файлы **User.dat и System.dat** по той или иной причине будут повреждены. Каждый раз при загрузке персонального компьютера Windows автоматически обновляет эти резервные копии, копируя текущие файлы реестра в файлы с расширением **da0.** Теоретически это позволяет вам всегда иметь **на** своем компьютере новейшую (последнюю) информацию о загрузочной конфигурации (Last-best-boot-Configuration).

Однако файлы **da0** не являются абсолютно надежной защитой от системных проблем. Так, в случае повреждения файлов **User.dat** и (или) **System.dat** файлы **da0** хотя и можно использовать для воссоздания файлов **dat**, но возможна ситуация, когда поврежденными оказываются и файлы **da0.** Поэтому рекомендуется иметь несколько резервных копий всех четырех файлов реестра **(System.dat, User.dat, System.da0, User.da0)** и хранить их в разных местах (например, в отдельных каталогах жесткого диска и на дискетах).

При копировании файлов **dat и da0** при загруженной системе Windows'95 вы можете встретиться с проблемами.

Если это случится, воспользуйтесь программ-оболочкой **Norton-Commander** (или аналогичной ей) для работы с операционной системой DOS. В каталоге **C:\Windows** найдите нужные файлы **(System.dat, User.dat, System.da0, User.da0)** и снимите с них атрибуты скрытых и системных файлов. После этого вы легко сможете сделать необходимые копии.

В процессе инсталляции Windows'95 система предлагала вам создать так называемую **загрузочную дискету.** Если в тот момент вы проигнорировали это предложение, то вам придется сделать это сейчас.

Для ее создания необходимовыполнить следующие операции:

>• выберите опцию Свойства: **Установка и удаление программ** (Add/Remove Programs) из **Панели управления** (Control Panel) и выполните щелчок мышью на вкладке **Системный диск** (Startup Disk);

>• вставьте дискету в дисковод (A) на компьютере, но помните, что при создании загрузочной дискеты все данные, которые содержались на ней ранее, будут уничтожены;

>• нажмите кнопку **Создать диск** (Create Disk) и далее следуйте инструкциям, появляющимся на экране.

Пометьте дискету как загрузочную. Скопируйте на нее все важные системные файлы (например, основные драйверы, файлы паролей PWL и все

файла сетевой конфигурации, имеющиеся на вашей системе).
Еще раз обращаем внимание на то, что нельзя забывать периодически делать резервные копии и ваших рабочих файлов. Это необременительная процедура. Однако рано или поздно наступит момент, когда вы высоко оцените свою прозорливость или горько пожалеете об обратном.

**Восстановление поврежденного реестра**

Если реестр все же оказался поврежденным в результате допущенных ошибок при его редактировании или вследствие специфических проблем с Windows'95 и возникла ситуация, когда система не может загрузиться, то необходимо предпринять меры по его восстановлению.
В этом случае попробуйте выполнить восстановление одним из следующих способов.
1. Выполните операцию по передаче управления от файла **System.dat** файлу **System.daO.**
С этой целью перезагрузите компьютер и нажмите клавишу **F8** сразу же после появления строки **Starting Windows'95...**
На экране появится стартовое меню. Выберите из него опцию **Command prompt only** (только командная строка). При этом на экране отобразится командная строка MS-DOS (этого же эффекта можно добиться, если в момент загрузки нажать клавиатурную комбинацию **<Shift> + <F5>).** В ряде случаев, обнаружив неполадки в системе (в процессе неудачной загрузки), компьютер сам выйдет в состояние командной строки.
Введите следующие команды:

```
C:\>cd\nc                                                    (*)
C:\NC>nc
```

Это приведет к раскрытию панелей программ-оболочки **Norton-Commander, с** помощью которой вы легко сможете переименовать испорченные файлы **System.dat и User.dat в System.bad и User.bad**, а файлы **System.daO и User.daO**, соответственно, в **System.dat и User.dat.** В случае возникновения проблем с переименованием снимите атрибуты скрытых и системных файлов.
Используя функциональную клавишу **F10**, вернитесь в командную строку MS-DOS и комбинацией клавиш **<Ctrl> + <Alt> + <Del>** перезагрузите компьютер.
Данную процедуру можно выполнить и без использования **Norton-Commander**, необходимо только ввести в командной строке MS-DOS следующие управляющие команды:

```
C:\> attrib — r — h — s system.dat
C:\> attrib — r — h — s system.da0
C:\> ren system.dat system.bad
C:\> ren system.daO system.dat
C:\> attrib — r — h — s user.dat
C:\> attrib — r — h — s user.da0
C:\> ren user.dat user.bad
C:\> ren user.daO user.dat
```

и после этого перезагрузить компьютер (**<Ctrl> + <Alt> + <Del>).** Эта процедура должна восстановить реестр в том состоянии, в котором он находился, когда вы последний раз успешно загрузили Windows'95. Если желаемый результат не достигнут, то перейдите ко второй операции.
2. Попытайтесь загрузить систему с загрузочной дискеты **(Emergency recovery disk).**
Для этого в процессе начального тестирования компьютера войдите в **меню установок CMOS** способом, рассмотренным в п. 1.6.
В разделе **BIOS FEATURES SETUP** выберите функцию **Boot Sequence и с** помощью клавиш **PgUp и PgDn** установите такую последовательность устройств, на которых компьютер ищет операционную систему, чтобы имя дисковода гибкого диска (А) стояло первым в ряду, например **A,C,SCSY.**

Вставьте загрузочную дискету в дисковод (A). Выйдите из меню с сохранением всех установок. Компьютер автоматически повторит процесс тестирования и загрузки.
После завершения начального этапа появится командная строка. Введите уже известные вам команды (**) из способа 1 и перезагрузите компьютер. Эта процедура также должна восстановить реестр в состоянии последней успешной загрузили Windows'95.
Если снова желаемого результата достигнуть не удалось, то это означает, что поврежденными оказались и файлы с расширением **da0** и операцию восстановления придется продолжить.
3. Замените в каталоге **C:\Windows** испорченные файлы на имеющиеся копии.
С этой целью перезагрузите компьютер и описанным выше путем раскройте панели программ-оболочки **Norton-Commander**. С ее помощью замените в каталоге испорченные файлы **(System.dat, User.dat, System.daO и User.daO)** на их резервные копии, которые, следуя нашим инструкциям, вы приготовили заранее и хранили на специальной дискете.
С использованием функциональной клавиши **F10** вернитесь в командную строку MS-DOS и комбинацией клавиш **<Ctrl> + <Alt> + <Del>** перезагрузите компьютер.
Если же и в этот раз не удалось достигнуть положительного результата, то это серьезный аргумент в пользу того, что с вашим компьютером большие проблемы, но можно попробовать исправить положение, воспользовавшись следующим способом.
4. Загрузите компьютер в безопасном режиме.
Для этого перезагрузите компьютер и нажмите клавишу **F8** сразу же после появления строки **Starting Windows'95...**
На экране появится стартовое меню, с одной из опций которого вы уже знакомы **(Command prompt only)**. Однако всего таких опций восемь, и так как при русификации Windows'95 их значения не переводились, то раскроем их в табл. 2.6.1.
Для исправления ошибок реестра целесообразно выбрать опцию **Safe Mode**, так как она позволяет загрузить систему в обход реестра и стартовых файлов **Autoexec.bat и Config.sys**. Фактически Windows загружает только стандартные драйверы мыши, клавиатуры и стандартного дисплея VGA, графическая оболочка устанавливает разрешение 640x480 пикселей.

**Таблица 2.6.1. Значение опций стартового меню операционной системы Wintlows'95**

№ п/п /Название опции /Выполняемая операция

1 /Normal /Повторяет попытку нормального запуска Windows'95 с загрузкой всех драйверов устройств и параметров реестра

2 /Logget (\bootlog.txt) /Осуществляет загрузку Windows'95 с формированием в корневом каталоге системного диска (C) файла Bootlog.txt, который содержит запись протокола загрузки системы. Этот файл может быть использован для анализа всех загруженных и инициализированных драйверов и просмотра и статуса каждого из них. (Файл читается с использованием функциональной клавиши F3.)

3 /Safe Mode /Запускает Windows'95 в безопасном режиме без обработки инициализированных файлов. Используется только базовый набор драйверов в обход реестра и стартовых файлов Autoexec-bat и Config-sys. В безопасном режиме Windows '95 можно также запустить, если в процессе загрузки нажать клавишу F5 или ввести из командной строки команду WIN /D:M

4 /Safe Mode with Network Support /Запускает Windows'95 в безопасном режиме в обход стартовых файлов. Используются только базовые драйверы, включая базовые сетевые драйверы. В безопасном режиме Windows '95 можно также запустить, если в процессе загрузки нажать клавишу F6 или ввести

из командной строки команду WIN /D:N

5 /Step-by-step Confirmation /Позволяет вам давать подтверждение на запрос обработки каждой строки из начальных файлов, включая Autoexec.bat и Config.sys. На вопросы о строках, которые Вы хотите обрабатывать, отвечайте Y; а о строках, обработку которых Требуется обойти, отвечайте N. Эту опцию можно запустить, если нажать клавишу F8 при появлении на экране стартового меню

Окончание табл. 2.6.1

№ I1.IL /Название опции /Выполняемая операция

6 /Command prompt only /Запускает MS-DOS (версии Windows'95) с обработкой стартовых файлов и реестра, отображая только командную строку MS-DOS

7 /Safe Mode command prompt only /Запускает MS-DOS (версии Windows'95) в безопасном режиме и отображает только приглашение ввести командную строку в обход стартовых файлов. Этого же эффекта можно добиться, если в момент загрузки нажать клавишную комбинацию <Shift>+<F5>

8 /Previous version of MS-DOS i /Запускает предыдущую версию MS-DOS, если ваша конфигурация предусматривает загрузку различных операционных систем. Для того чтобы эта опция была доступна, в процессе инсталляции Windows'95 необходимо указать другой каталог для установки, отличающийся от предложенного по умолчанию. Кроме того, в файле MSDOS.SYS должно быть установлено BootMulty=1. Эту опцию можно запустить путем нажатия клавиши F4 при загрузке системы

Так как в этом режиме реестр Windows'95 не активен, то вы легко можете получить доступ к конфигурационным файлам и модифицировать их параметры.

После внесения необходимых изменений перезапустите Windows'95 в нормальном режиме.

При отсутствии положительных результатов у вас, видимо, остались только способы 5 и 6.

5. Попытайтесь восстановить операционную систему в том виде, как она выглядела после первоначальной инсталляции Windows'95.

Действуя так, как это было описано в способе 3, раскройте панели программ-оболочки **Norton-Commander** и отыщите в корневом каталоге системного диска (C) файл **System.lst**, созданный при запуске программы **Windows'95 Setup**. В нем содержится информация о вашей системе на момент первого

запуска программы Windows'95. Замените этим файлом файл **System.dat** в директории **C:\ Windows** и перезагрузите компьютер.

6. Полностью переустановите операционную систему на компьютере.

### 2.6.3. Защита от заражения компьютерными вирусами

В наше время никого уже не надо убеждать в необходимости защиты информации, хранящейся и обрабатываемой в компьютере, от вирусов. Однако далеко не все знают, что и как нужно делать, чтобы защитить свою информацию от возможных деструктивных последствий.

История возникновения проблемы связана с именем Фрэда Коэна (Fred Cochen), известного специалиста в области компьютерной безопасности, научного сотрудника Лехайского университета.

Работая над проблемой защиты от несанкционированного копирования программного продукта, Коэн написал небольшую программу, которая обладала способностью к быстрому самовоспроизведению и совершению различных негативных действий: стиранию важной информации на системном диске, уничтожению файлов, изменению переменных в операционной системе ЭВМ и т. д. Программа активизировалась в случае незаконного копирования

исходной авторской программы. Им же были проведены первые серьезные работы, посвященные математическим исследованиям жизненного цикла и механизма размножения компьютерных вирусов.
Работа Коэна была опубликована в материалах 7-й Национальной конференции США по компьютерной безопасности, состоявшейся в 1984 году. В то время это выступление не нашло отклика у специалистов по компьютерной безопасности, которые не придали сообщению большого значения. Однако уже в 1985 году стали появляться сообщения о реальных фактах проявления компьютерных вирусов.
В современном понимании **компьютерный вирус** — это специально написанная небольшая по размерам программа, которая может «приписывать» себя к другим программам, то есть «заражать» их, а также выполнять различные нежелательные действия (например, портить файлы или таблицу размещения файлов, «засорять» оперативную память и т. д.).
Характерной особенностью воздействия вирусов на компьютерную систему, отличающей ее от других видов потенциально опасных воздействий, является то обстоятельство, что происхождение вирусов имеет преднамеренный характер, а попадание в конкретный компьютер, как правило, случайный.
Одна из причин, из-за которых стало возможным такое явление, как компьютерный вирус, — это отсутствие эффективных универсальных способов защиты. В связи с последним обстоятельством различные фирмы и программисты постоянно работают над созданием средств, восполняющих указанный недостаток.
Как результат, в современных вычислительных системах реализовано огромное количество аппаратных и программных методов защиты.
К простейшим аппаратным методам относится, например, блокировка возможности записи на гибкий диск путем закрытия (заклеивания) отверстия защиты от записи. Это достаточно эффективный способ, но применение его распространяется только на особо важные дискеты, несущие неизменяемую информацию (копии системных файлов, идентификационные признаки и т. п.).
Более сложным аппаратным методом является применение специальных дополнительных плат, устанавливаемых в компьютер и выполняющих функции контроля зараженности системных файлов, загрузочных (boot) секторов, опасных действий с портами жестких и гибких дисков, попыток записи в память CMOS. Строго говоря, это* уже не аппаратный, а программно-аппаратный метод, который все же вытесняется программными методами в связи с быстрым развитием компьютерных технологий и, в частности, с существенным увеличением оперативной памяти, что делает неактуальным применение дополнительных устройств.
К основным видам программных методов защиты можно отнести следующие:
>• использование специальных резидентных программ в оперативной памяти компьютера;
**>•** установка атрибутов «Только для чтения» (Read Only) на отдельные области памяти и файлы;
>• проведение тестирований на наличие вирусов;
>• архивирование.
Использование резидентных программ — один из эффективных методов, основанный на применении специальных программ, которые постоянно находятся в оперативной памяти (являются «резидентами») и перехватывают все запросы к операционной системе на выполнение различных «подозрительных» действий, то есть операций, которые используют компьютерные вирусы для своего размножения и порчи информации в компьютере.
При каждом запросе на такое действие на экран монитора выводится сообщение о том, какое действие затребовано и какая программа желает

его выполнить. Пользователь может разрешить либо запретить его выполнение.
Достоинством такого способа является возможность свести к минимуму возможные потери, так как он позволяет обнаруживать вирус на ранней стадии, когда тот еще не успел размножиться и совершить разрушающие действия. Но способ не лишен и недостатков. Прежде всего резидентная программа защиты от вирусов постоянно занимает часть оперативной памяти, что, естественно, к достоинствам не отнесешь. Кроме того, при частых запросах отвечать на них может надоесть даже самому терпеливому пользователю. И наконец, имеются виды вирусов, работа которых не обнаруживается резидентными программами защиты, впрочем этот недостаток характерен для любой антивирусной программы.
Установка атрибутов «Только для чтения» (Read Only) на отдельные области памяти и файлы позволяет защитить операционную систему и наиболее важные файлы от заражения. С этой целью необходимо провести несколько операций.
1. При помощи специальных программ разбить жесткий диск на несколько частей — условных логических дисков, например на два. Один или несколько логических дисков отвести для хранения изменяемых программ и данных, а другой (другие) с защитой от записи — только для программ и данных, которые будут использоваться, но не изменяться.
2. Защитить от записи CMOS-память системной BIOS.
Дело в том, что одной из возможных модификаций компьютера является обновление системной BIOS. Ранее эта процедура требовала обязательной ее физической замены на материнской плате, но примерно с 1994 года стали предлагаться обновленные версии, так называемые flash BIOS, которые можно просто стирать и перезаписывать.
Однако это удобство таит в себе и серьезную опасность: возможность заражения BIOS компьютерными вирусами и, как следствие, невозможность загрузки операционной системы. Так, именно система BIOS, как один из объектов для нанесения удара, использована в вирусе, получившем название «Чернобыльский» по дате своей первой активизации (26 апреля 1999 года). По этой причине раздел **BIOS FEATURES SETUP** меню **установок CMOS** (см. п. 1.6) содержит функцию **Virus Warning** (Защита от вирусов). Она предохраняет загрузочный сектор (boot sector) CMOS и таблицу разделов (partion table) жесткого диска от инфицирования программами-вирусами.
По умолчанию (при первоначальной поставке компьютера) эта функция **«Disabled»** (отключена) и имеется возможность записи в указанные разделы.
Для того чтобы активизировать систему защиты, необходимо перевести опцию **Virus Warning** (Защита от вирусов) в состояние **«Enabled»** (активна), воспользовавшись для этого клавишей **PgUp** или **PgDn.**
В последнем случае функционирование компьютера приостанавливается при попытке изменения вышеуказанных разделов и появляется предупредительное сообщение. Пользователь при этом должен принять решение: санкционировать доступ к указанным разделам или прекратить выполнение задачи, чтобы с помощью антивирусного программного обеспечения проверить компьютер на инфицированность.
Однако при инсталляции Windows'95 указанная настройка **BIOS** может доставить вам некоторые проблемы; например, установка Windows'95 может не стартовать нормальным путем. Для того чтобы разрешить сложившуюся ситуацию, необходимо блокировать функцию защиты загрузочного сектора **CMOS.**
3. Установить атрибуты «Только для чтения» (Read Only) на наиболее важные файлы. Для этой цели с помощью меню кнопки «Пуск» (Start) откройте окно «Проводник» (Explorer) Панели задач. Выберите по очереди

файлы, которые хотите защитить от записи, и щелкните по ним правой кнопкой мыши. В раскрывшемся меню выберите опцию «Свойства» и войдите в нее. Установите атрибут «Только для чтения».

Проведение тестирований на наличие вирусов включает в себя как входной контроль всех поступающих программных продуктов, так и периодический контроль жесткого диска.

Практически во всех руководствах по защите компьютерной информации первым пунктом всегда присутствует предупреждение о неиспользовании программного обеспечения с других компьютеров и нелицензионных источников. Трудно что-либо возразить против этого предупреждения, однако реалии нашей жизни таковы, что для многих пользователей основной вид поступлений новых прикладных программ — это товарищеский обмен и пиратские компакт-диски, со всеми вытекающими отсюда последствиями, включая компьютерные вирусы. И ситуацию вряд ли исправит тот факт, что именно нелицензионные компакт-диски явились путем распространения вышеупомянутого «Чернобыльского» вируса. Хотя справедливости ради надо отметить, что в истории известны случаи, когда вирусы распространялись и в лицензионных запечатанных дисках прямо с завода-изготовителя.

Поэтому независимо от вида носителя и источника программного продукта подвергайте все программные изделия входному контролю!

Существуют три основных вида антивирусных программ: программы-фильтры; программы-вакцины; программы-фаги.

Программы-фильтры (иногда их называют программы-детекторы) проверяют, имеются ли в файлах на указанном пользователем диске специфические для определенных вирусов комбинации байтов.

Программы-вакцины имитируют сочетание условий, в которых должен заработать тот или иной тип вируса и проявить себя. Их применение позволяет выявлять вирус на ранней стадии — до того как он начал функционировать обычным путем, поэтому программы-вакцины часто используют в качестве резидентных программ.

Программы-фаги предназначены для удаления конкретных вирусов из зараженных программ, кроме того, они выполняют с зараженными файлами действия, обратные тем, которые производятся вирусом при заражении файла. То есть они делают попытку восстановления (лечения) зараженных файлов. Если это не удается, то файлы считаются неработоспособными и, как правило, удаляются.

Необходимо отметить, что следует стараться избегать одновременного использования фагов и вакцин. Дело в том, что вакцина тем качественнее, чем более точно она имитирует вирус. Но из этого следует, что многие антивирусные программы будут принимать эти вакцины за настоящие вирусы. Возможно даже, некоторые фаги попытаются обезвредить эти вакцины. Ведь в «представлении» фагов вакцины — это настоящие вирусы. Это противоречие может привести к нарушению нормальной работы операционной системы.

Уже отмечалось, что, к сожалению, отсутствуют универсальные антивирусные средства, поэтому любая антивирусная программа работает только с известными ей типами вирусов, общее количество которых обычно указывается в описании к соответствующей программе. Поэтому если вы приобрели новый программный продукт, то, вероятнее всего, он имеет «знания» о большем числе вирусов, чем ваш предыдущий инструмент. Используйте новую антивирусную программу для тестирования жесткого диска компьютера на наличие пропущенных при входном контроле вирусов.

Архивирование — не менее важное средство защиты от вирусов, чем все предыдущие. Другие методы заменить его не могут, так как архивирование — это создание копий используемых файлов, которые окажутся незаменимыми в том случае, если вы обнаружите, что рабочие файлы заражены и не поддаются лечению.

Делайте архивирование регулярно, используя для этих целей специально разработанные программы-архиваторы, которые позволяют существенно экономить место на архивных дискетах. Не забывайте делать копии и с файлов реестра. Их резервирование важно не только как средство защиты от вирусов, но и необходимо на случай аварийных ситуаций, связанных с ошибками пользователей.

### 2.6.4. Программно-аппаратные средства защиты информации от несанкционированного доступа

Условно все современные программно-аппаратные средства защиты информации можно разделить на три основные группы:

А. Средства, разработанные для защиты информации от НСД в информационных сетях, но допускающие применение и в персональных компьютерах;

Б. Средства, принципиально применимые только в компьютерных сетях и предназначенные для разделения информационных потоков, — так называемые межсетевые экраны;

В. Средства, принципиально предназначенные для защиты информации от НСД в персональных компьютерах.

Рассмотрим их более подробно.

**А. Средства защиты информации в информационных сетях**

В так называемой группе А к наиболее известным программно-аппаратным средствам относятся:

>• система защиты от НСД «Спектр-Z»;
>• система Secret Net;
>• программно-аппаратный комплекс защиты **DAALLAS LOCK**;
>• программно-аппаратная система «Криптон-Вето»;
>• система криптографической защиты информации «Верба-0»;
>• криптографический комплекс «Шифратор IP потоков» **(ШИП).**

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА «СПЕКТР-Z»

**Спектр-Z** — это комплексная система защиты, устанавливаемая на различные по классу ПЭВМ типа IBM PC (настольные, портативные, переносные), работающие под управлением операционных систем Windows'95 или Windows'98 всех версий.

**Спектр-Z** по своим характеристикам соответствует требованиям руководящих документов (РД) Гостехкомиссии России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» по 3-му классу защищенности и «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»!») классу защищенности 1В, а также требованиям технических условий № ТУ 4012-001-13194780-99.

Система сертифицирована в 1999 г. Гостехкомиссей при Президенте РФ. Сертификат соответствия №251. Основные возможности системы **Спектр-Z:**

>• обеспечение защиты от НСД широкого круга современных и проектируемых программных комплексов и баз данных без дополнительных трудозатрат на разработку средств защиты в рамках каждого отдельного проекта, как для автоматизированной системы на базе отдельной рабочей станции, так и в рамках автоматизированной системы на базе локальной сети;
>• создание защищенного рабочего места для работы с Internet;
>• обеспечение управления полномочиями пользователей (полный доступ, только чтение, нет доступа, режим преобразования) для логических дисков;
>• блокировка клавиатуры, монитора и мыши при отсутствии зарегистрированного пользователя;
>• ограничение работы пользователя заданным множеством дискет, сформированных администратором безопасности;

>• обнаружение атаки компьютерных вирусов и случайных или преднамеренных искажений программ и данных;
>• учет работы пользователей на компьютере.

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА SECRET NET

**Система Secret Net**. Предназначена для защиты информации, хранимой и обрабатываемой в локальных вычислительных сетях под управлением операционной системы Novell NetWare.

Версия 2.1 системы сертифицирована в 1996г. Гостехкомиссей при Президенте РФ (сертификат соответствия №38) по классу защищенности «3» и может быть использована для зашиты информации в автоматизированных системах до класса 1В включительно.

Базовая версия системы позволяет защищать как автономные компьютеры, так и рабочие станции локальной сети, работающие под управлением ОС MS-DOS (Pt-DOS) 3.30-6.22, Windows 3.xx и Windows for Workgroups, Novell NetWare (v3.1X и 4.X).

Версия 3.0 системы сертифицирована в 1997г. Гостехкомиссей при Президенте РФ (сертификат соответствия № 80) по классу защищенности «3» и также может быть использована для зашиты информации в автоматизированных системах до класса 1В включительно.

Эта версия системы позволяет обеспечить защиту хранимой и обрабатываемой информации в сетях Novell NetWare с PC под управлением не только MS-DOS и Windows 3.11, но и Windows'95 for Workgroups, Novell NetWare (v3.1X и 4.X).

В 1997 г. была создана и сертифицирована по 3-му классу система Secret Net NT для работы в ЛВС на основе сетевой ОС Windows NT.

Система **Secret Net** обеспечивает:

>• аутентификацию пользователей при помощи специальных аппаратных средств (Touch Memory и Smart Card) при возможности расширения номенклатуры используемых аппаратных средств аутентификации;
>• дискреционное (избирательное) управление доступом пользователей к данным, хранимым на локальных дисках компьютеров, а также к различным устройствам (принтерам, коммуникационным портам);
>• полномочное (мандатное) управление доступом как к локальным, так и к сетевым файлам и каталогам с использованием трех степеней конфиденциальности (общедоступная, конфиденциальная и строго конфиденциальная);
**>•** подключение средств криптографической защиты данных;
**>•** подробную регистрацию событий, происходящих в системе и имеющих отношение к ее безопасности, а также гибкое управление регистрацией;
>• постепенное (при необходимости) включение механизмов защиты;
>• динамическое присвоение пользователям полномочий по доступу к сетевым ресурсам при запуске программ;
>• централизованное управление средствами защиты;
>• оперативный контроль (мониторинг) за работой пользователей;
>• контроль целостности программ, используемых ОС и пользователем;
>• гибкость настройки и простоту в эксплуатации системы.

Существуют различные модификации системы **Secret** Net, например **Secret Net NT** или **Secret Net Win.**

**Система Secret Net NT** предназначена для обеспечения защиты информации в ЛВС на основе сетевой ОС Windows NT. Она обеспечивает:

>• аутентификацию пользователей при помощи специальных аппаратных средств (Touch Memory и Smart Card);
>• полномочное управление доступом пользователям к данным;
>• возможность подключения средств криптографической защиты данных как передаваемых по локальной сети, так и хранимых на магнитных дисках;
>• централизованное управление доступом пользователей к совместно используемым ресурсам (каталогам и принтерам);

>• оперативный контроль (мониторинг) за работой пользователей;
>• оповещение администратора безопасности о событиях НСД;
>• подробную регистрацию событий, происходящих в системе и имеющих отношение к ее безопасности, а также гибкое управление регистрацией;
>• централизованный сбор и анализ содержимого системных журналов;
>• контроль целостности программ, используемых ОС и пользователем.

Для сетей Windows NT разработаны как клиентский вариант, устанавливаемый на рабочей станции, так и сервер управления доступом, устанавливаемый либо на контроллере домена, либо на рабочей станции сети.

**Система Secret Net Win** предназначена для обеспечения защиты информации в локальных вычислительных сетях на основе Windows'95. Secret Net Win обеспечивает:

>• аутентификацию пользователей при помощи специальных аппаратных средств (Touch Memory и Smart Card);
>• избирательное (дискреционное) разграничение доступа пользователям к каталогам, файлам и системам, в том числе и в одноранговой сети;
>• полномочное управление доступом пользователям к данным;
>• поддержку централизованного управления доступом пользователей к совместно используемым данным;
>• оперативный контроль (мониторинг) за работой пользователей;
>• подключение средств криптографической защиты данных;
>• оповещение администратора безопасности о событиях НСД;
>• подробную регистрацию событий, происходящих в системе и имеющих отношение к ее безопасности, а также гибкое управление регистрацией.

Существует клиентский вариант **Secret Net Win** для работы с серверами управления доступом на платформах Windows NT и Novell NetWare.

**Secret Net Remote Tools** — Специальное программное средство, предназначенное для управления удаленными рабочими станциями в сети Novell NetWare, оснащенными системой Secret Net. Она позволяет:

>• с разрешения администратора системы устанавливать удаленное соединение с рабочими станциями как собственной локальной сети, так и любой другой локальной сети на основе ОС Novell NetWare, с которой есть связь по протоколу TCP/IP и в которой присутствует сервер управления доступом системы Secret Net;
>• подключать средства криптографической защиты для шифрования данных, передаваемых по каналу связи;
>• просматривать содержимое экрана (только текстовые режимы) и управлять клавиатурой рабочей станции сети.

Данное программное средство функционирует в среде ОС MS-DOS и Novel NetWare.

Осуществление аутентификации пользователей осуществляется с помощью аппаратных средств:

**Secret Net Card** — обеспечивает ввод имени и пароля пользователя до загрузки ОС, а также управление загрузкой компьютера с гибких магнитных дисков.

**Secret Net TM Card** — выполняет функции Secret Net Card, а также обеспечивает аутентификацию пользователя при помощи Touch Memory.

**Secret Net Smart Card —** выполняет функции Secret Net Card, а также обеспечивает аутентификацию пользователя при помощи Smart **Card.**

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС ЗАЩИТЫ DAALLAS LOCK

**Версия DAALLAS LOCK 4.1.** Предназначена для работы в операционной среде Windows'95. Система защиты сертифицирована Государственной технической комиссией по 3-му классу защищенности (сертификат № 181 от 02.06.98).

Программное обеспечение содержит:

>• модуль контроля целостности;

>• встроенную антивирусную защиту;
>• возможность назначения пользователю списка разрешенных и запрещенных задач;
>• регистрация событий, относящихся к доступу к компьютерной информации;
>• блокировка экрана и клавиатуры в отсутствие пользователя.
Аппаратная часть содержит:
>• в качестве основного средства идентификации — электронную карту iButton (Touch Memory*);
>• контроллер КТ-331, содержащий собственный процессор, флэш-память и ROM-BIOS; он позволяет обеспечивать выполнение процедуры опознания пользователя на любом ПК, независимо от типа ОС и совместимость с любым ПО.
Особенности сетевой версии:
>• вход в сеть по электронной карте Touch Memory;
>• удаленная работа с матрицами доступа: сравнение, изменение, обновление базы;
>• просмотр на мониторе администратора безопасности экранов подключенных рабочих станций в режиме реального времени;
>• графическое отображение топологии сети;
>• эмуляция клавиатуры удаленной рабочей станции;
>• просмотр списков пользователей и журналов любых рабочих станций с установленным комплексом DAALLAS LOCK;
>• оперативная блокировка действий пользователей рабочих станций в критических ситуациях.
**Версия DAALLAS LOCK 5.0.** Система предназначена для работы на любом IBM-совместимом компьютере под управлением ОС Windows NT Workstation. Позволяет поддерживать работу до 32 зарегистрированных пользователей.
Основное отличие от версии 4.1. — наличие инструмента Secure File Deletion, позволяющего гарантированно стирать уничтоженные файлы путем затирания их места на диске нулевым кодом.
ПРОГРАММНО-АППАРАТНАЯ СИСТЕМА «КРИПТОН-ВЕТО»
**Система «Криптон-Вето»** предназначена для защиты ПК с процессором не ниже 386 под управлением MS DOS и выше. Windows 3.1, Windows'95. Персональный компьютер при этом может использоваться в качестве:
>• абонентского пункта;
>• центра коммутации пакетов;
>• центра выработки ключей.
Система ограничивает круг лиц и их права по доступу к информации на персональном компьютере. Ее реализация основана на технологиях «прозрачного» шифрования логических дисков по алгоритму ГОСТ 28147-89 и электронной цифровой подписи по ГОСТ 34.10/11-94. Система сертифицирована по классу 1В (сертификат № 178 от 29 апреля 1998 г.) по требованиям Гостехкомиссии РФ к защищенности автоматизированных систем от несанкционированного доступа.
Основные функции программно-аппаратной системы «Криптон-Вето»:
>• обеспечение защищенности информации в случае кражи жесткого диска или ПК;
>• обеспечение защиты от несанкционированного включения компьютера;
>• разграничение полномочий пользователей по доступу к ресурсам ПК;
>• проверка целостности используемых программных средств в момент - включения системы;
>• проверка целостности программы в момент ее запуска на выполнение;
>• запрещение запуска на выполнение посторонних программ;
>• обеспечение «прозрачного» шифрования информации при обращении к защищенному диску;
>• обнаружение искажений, вызванных вирусами, ошибками пользователей,

техническими сбоями или действиями злоумышленника.
Основным аппаратным элементом системы является серийно выпускаемая и аттестованная ФАПСИ плата КРИПТОН-4, с помощью которой проверяется целостность системы и выполняется шифрование по ГОСТ 28147-89.
Принцип работы программно-аппаратной системы заключается в следующем.
Жесткий диск разбивается на логические диски. Первый логический диск (С) отводится для размещения системных программ и данных. Последний — под систему защиты от НСД и доступен только администратору. Остальные логические диски предназначены для хранения информации и программ пользователей. Эти диски можно разделить по степени конфиденциальности защищаемой информации. Функции администратора заключаются в определении степени конфиденциальности информации на каждом из логических дисков и определении круга лиц, имеющих доступ к этим дискам.
По форме хранения информации диски подразделяются на открытые и шифруемые; по виду доступа;
>• доступные для чтения и записи;
>• доступные только для чтения;
>• недоступные (заблокированные).
Недоступный диск не виден обычному пользователю (в DOS), а следовательно, и не провоцирует его на несанкционированный доступ к информации. Для шифрования информации на каждом логическом диске используется свой ключ.
Для разграничения полномочий администратор формирует список пользователей, в котором указывает:
>• идентификатор пользователя;
>• уровень доступа к конфиденциальной информации;
>• права доступа к логическим дискам.
Для исключения возможности установки на ПК посторонних программ администратор определяет перечень программных продуктов, разрешенных к запуску на данном компьютере. Разрешенные программы подписываются им методом электронной цифровой подписи.
Для аутентификации пользователей используются:
>• пароль;
>• специальные ключи, выполненные в виде ключевой дискеты, электронной карточки (смарт-карты) или таблетки (Touch-Memory).
С целью исключения загрузки ПК в обход системы защиты загрузка осуществляется только с жесткого диска. При включении компьютера (до загрузки операционной системы) с «винчестера» аппаратно проверяется целостность ядра системы безопасности, системных областей жесткого диска, таблицы полномочий пользователей. Затем управление передается проверенному ядру системы безопасности, которое, в свою очередь, проверяет целостность операционной системы. В процессе работы ПК загружаются ключи только тех дисков, к которым пользователю разрешен доступ.
Для протоколирования процесса работы ведется Журнал, просмотр которого возможен только администратором. Для защиты информации от просмотра администратором пользователь может закрыть ее средствами абонентского шифрования.
СИСТЕМА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ «ВЕРБА-0»
**Система криптографической защиты информации** (СКЗИ) представляет собой программно-аппаратный комплекс, предназначенный для ЗИ при ее хранении и передаче по каналам связи.
СКЗИ «Верба-0» решает следующие задачи:
>• шифрование/расшифрование информации на уровне файлов;
>• генерацию электронной цифровой подписи (ЭЦП);
>• проверку (ЭЦП).
Система поставляется в следующих основных вариантах:

>• в виде автономного рабочего места;
>• в виде модулей, встраиваемых в ПО заказчика.
СКЗИ «Верба-0» в различных модификациях функционирует под управлением операционных систем MS DOS v.5.0 и выше, Windows'95, Windows NT, UNIX (HP UX) на персональных ЭВМ, совместимых с IBM PC/ AT. Требуемый объем оперативной памяти не более 155 кбайт. Кроме того, необходим накопитель на гибком магнитном диске.
Алгоритм шифрования выполнен в соответствии с требованиями ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая».
Цифровая подпись выполнена в соответствии с требованиями ГОСТ Р34.10-94 «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма».
Функция хэширования выполнена в соответствии с требованиями **ГОСТ** Р34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования».
Ключи шифрования симметричные, ключи для ЭЦП — асимметричные.
При обработке информации на ПЭВМ СКЗИ «Верба-0» обеспечивает следующие показатели.
СКЗИ «Верба-0» имеет сертификат ФАПСИ №124-0264 от 10.04.99 г.
**Таблица 2.1.**
Операции /PC/AT 486/33, ISA /PC/AT 486/100 VESA
Шифрование /200 Кб/с /520 Кб/с
Вычисление хэш-функции /120 Кб/с /330 Кб/с
Формирование ЭЦП /0,3с /0,04 с
Проверка ЭЦП /0,7с /0,2 с

КРИПТОГРАФИЧЕСКИЙ КОМПЛЕКС «ШИФРАТОР IP ПОТОКОВ» (ШИП)
**Криптографический комплекс «Шифратор IP потоков»** предназначен для решения следующих вопросов:
>• обеспечение конфиденциальности и целостности информации, передаваемой в сетях общего пользования;
>• создание защищенных подсетей передачи конфиденциальной информации;
>• объединение локальных вычислительных сетей в единую защищенную сеть;
>• закрытие доступа к ресурсам локальной сети или отдельных компьютеров из сети общего пользования;
>• организация единого центра управления защищенной подсетью.
Криптографический комплекс «ШИП» обеспечивает:
>• закрытие передаваемых данных на основе использования функций шифрования в соответствии с ГОСТ 28147-89;
>• контроль целостности передаваемой информации;
>• аутентификацию абонентов (узлов сети);
>• защиту доступа к локальной сети и закрытие IP адресов подсети;
>• создание защищенных подсетей в сетях общего пользования;
>• защиту от НСД ресурсов самого шифратора;
>• передачу контрольной информации в «Центр управления ключевой системой защищенной IP сети;
>• поддержку протоколов маршрутизации RIP II, OSPF, BGP;
>• фильтрацию IP, ICMP, TCP- соединений на этапе маршрутизации и при приеме/передаче в канал связи;
>• поддержку инкапсуляции IPX в IP (в соответствии с RFC-1234);
>• поддержку инкапсуляции IP в X.25 и Frame Relay.
Шифратор IP потоков содержит плату «Кулон» с интерфейсом ISA, используемую для защиты от НСД при загрузке системы и для получения от датчика случайных чисел последовательностей, необходимых для реализации процедуры шифрования.

Криптографический комплекс «ШИП» имеет сертификат ФАПСИ № СФ/124-0815 от 10.04.97 г.

**Б. Межсетевые экраны**

Межсетевой экран (МЭ) — это локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль информации, поступающей в автоматизированную систему и/или выходящей из нее.

В настоящее время на мировом рынке представлено более 50 различных межсетевых экранов, отличающихся платформами функционирования, функциональными возможностями и производительностью.

Функциональные требования к МЭ, используемым в РФ для защиты информации, регламентированы Руководящим документом (РД) Государственной технической комиссии при Президенте Российской Федерации «Межсетевые экраны. Защита от несанкционированного доступа к информации. Классификация межсетевых экранов и требования по защите информации» (см п.2.1.5).

На российском рынке сетевых средств защиты информации представлено более десяти МЭ, сертифицированных по требованиям Гостехкомиссии России (табл.2.6.2.).

Все они сочетают в себе возможности пакетной фильтрации и фильтрации на прикладном уровне. Краткие технические характеристики некоторых МЭ приведены в табл.2.6.3. В таблице не представлены МЭ, сертифицированные по схеме единичного экземпляра.

Естественно, что использование МЭ приводит к снижению производительности сети. Изменение пропускной способности различных МЭ в зависимости от нагрузки приведено на рис 2.6.2 на с. 780.

**В. Программно-аппаратные средства защиты конфиденциальной информации в персональном компьютере**

**Secret Disk.** Программно-аппаратное средство Secret Disk предназначено для защиты конфиденциальной информации на ПК, прежде всего типа Notebook.

Основные возможности:

>• защита данных осуществляется с помощью профессиональных алгоритмов шифрования;

>• генерация ключей самим пользователем;

**>•** двойная аутентификация пользователя (аппаратная и по паролю);

**Таблица 2.6.2. Сертифицированные межсетевые экраны**

Название межсетевого экрана /Класс защищенности в соответствии с руководящим документом (РД) и номер сертификата

МЭ «Пандора» версии 3.1.1 — СЗИ в сетях передачи данных по протоколу TCP/IP /Класс «ЗБ» по РД «АС» — № 73; Класс «З» по РД «МЭ» — № 183.

МЭ «Black Hole» версии BSDI-OS — автоматизированная система разграничения доступа /Класс «ЗБ» по РД «АС» — № 79; Класс «З» по РД «МЭ» — № 184.

МЭ «Застава» /Класс «З» по РД «МЭ» — № 145,155.

Аппаратно-программный комплекс «Застава-Джет» /Класс «2» по РД «СВТ» — № 146.

МЭ «Cyber Guard» версии 4.0 /Класс «З» по РД «СВТ» — № 171.

МЭ «AltaVista FireWall 97» /Класс «З» по РД «СВТ» —№173.

Аппаратно-программные комплексы на базе маршрутизаторов Bay Networks: Advanced Remote Node, Access Stack Node 2 (ASN2), BackBone Node (BN) /Класс «4» по РД «СВТ» — № 175.

Система защиты информации «FireWall-1» версии 3.Ob /Класс «4» по РД «СВТ» — № 190.

МЭ «FireWall-1/Plus for Windows NT» /Класс «4» по РД «СВТ» — № 194.

МЭ «Cisco FIX FireWall» /Класс «3» по РД «МЭ» — № 197, 222.

Программный комплекс «Межсетевой экран Застава-Джет-РС» /Класс «2» по РД «МЭ» — № 200.

Программный комплекс «Межсетевой экран FireWall-1/VPN-1» версии 4.0., Service Pack 2 /Класс «4» по РД «МЭ» — № 230.

Аппаратно-программный комплекс «МЭ WatchGuard»/Класс «4» по РД «МЭ» — № 236.

>• гашение экрана и блокировка клавиатуры при отключении идентификатора, нажатии заданной комбинации клавиш или длительной неактивности пользователя;

>• наличие режима работы под принуждением — в критической ситуации вводится специальный аварийный пароль, при котором система на некоторое время подключает секретный диск, стирает личный ключ шифрования и имитирует сбой операционной системы.

**Таблица 2.6.3. Технические характеристики некоторых видов МЭ**

Технические параметры и характеристики /МЭ «Black Hole» /МЭ «Cyber Guard» версии 4.0 /МЭ "AltaVista FireWall 97" /МЭ «Gauntlet»

Характеристики рабочей станции /В комплект поставки рабочая станция не входит. Рекомендуемая конфигурация: Pentium, 16Mb, HDD 0.8Gb, CDROM /В комплект поставки рабочая станция не входит. Рекомендуемая конфигурация: Pentium, 166, 64Mb, HDD 4Gb, CDROM /В комплект поставки рабочая станция не входит. Рекомендуемая конфигурация: PentiumII, 266, 128Mb, HDD 8Gb, CDROM/02 (Silicon Graphics); CPUR5000 180MHz PC; RAM 32Mb DIMM ECC; HDD 1.2Gb SCSI; 17' monitor

Операционная система /BSDIOS2.1 /UnixWare v.2.1 /Digital UNIX, Win NT /IRIXv.6.3

Производительность обработки /Зависит от конфигурации рабочей станции. Для вышеприведенной до 8,5Мбит/с /До 44 Мбит/с /До 60 Мбит/с /До 15 Мбит/с

Конфигурация DNS /Внешний DNS: на МЭ Внутренний DNS: в защищаемом сегменте на отдельной станции или на МЭ

Сетевые интерфейсы /Ethernet, Token Ring/Зависит от используемой платформы

Принцип работы Secret Disk заключается в создании дополнительного виртуального логического диска, который до завершения процесса аутентификации пользователя виден как обычный зашифрованный файл (например, с именем game.exe).

**Программный комплекс Кобра.** Он предназначен для установки на различные по классу ПЭВМ типа IBM PC, работающие под управлением MS DOS. Основные возможности:

>• осуществляет аутентификацию пользователей по паролю;

>• обеспечивает управление полномочиями пользователей по доступу к логическим устройствам A,B,C,… (полный доступ, только чтение, нет доступа, режим суперзащиты);

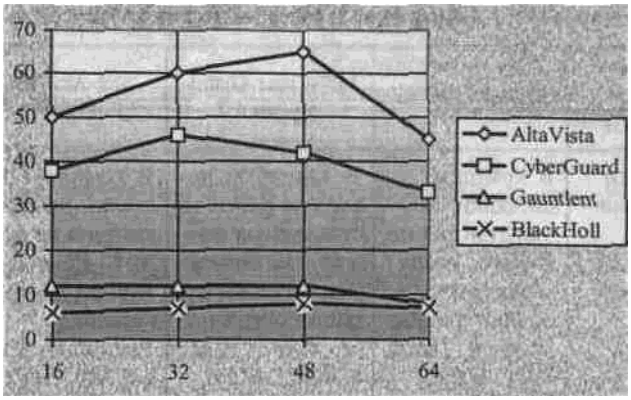



**Рис. 2.6.2. Изменение пропускной способности различных МЭ в зависимости от нагрузки**

**>•** ограничивает работу пользователя заданным множеством дискет;

**>•** санкционирует доступ к LPT и COM портам;

>• блокирует клавиатуру при неактивности зарегистрированного пользователя;

>• обнаруживает атаку компьютерных вирусов и случайные или преднамеренные искажения программ и данных;

>• выполняет автоматическое восстановление эталонной рабочей среды компьютера.

Программный комплекс сертифицирован Гостехкомиссей при Президенте РФ. Сертификат соответствия № 20. Также имеет свидетельство об официальной регистрации программ для ЭВМ № 950395 РосАПО.

**СГУ-1.** Система гарантированного уничтожения информации СГУ-1 (GIDS-1) предназначена для надежного уничтожения файлов и остаточной информации на магнитных носителях и в памяти ЭВМ. Принцип действия системы основан:

>• на уничтожении файлов путем записи по их физическим адресам затирающих последовательностей;

>• удалении сведений об имени файла и сто физическом расположении из каталога;

**>•** затирании незанятых кластеров;

**>•** многократном и комбинированном выполнении функций затирания.

Система сертифицирована в 1997г. Гостехкомиссей при Президенте РФ. Сертификат соответствия № 83.

## ЗАКЛЮЧЕНИЕ

Представленная книга не является исчерпывающим описанием всех возможных методов негласного получения информации с помощью технических средств разведки, а также способов противодействия. Да и не ставили авторы перед собой такую задачу. Это обусловлено следующими причинами:

>• динамичным изменением законодательства в области защиты информации;

>• бурным научно-техническим прогрессом в деле создания средств разведки и противодействия на базе микропроцессорной техники;

>• совершенствованием методик применения аппаратуры различного назначения;

>• закрытым характером существенной части информации в области защиты информации и противодействия разведкам (во всем мире это прерогатива спецслужб);

>• ограниченным объемом книги.

Что касается последнего, то авторы в ближайшее время планируют выпустить книги, посвященные отдельным вопросам правового, методического и технического обеспечения деятельности служб безопасности государственных и коммерческих предприятий по защите информации. В них будут детально рассматриваться относительно узкие вопросы применения той или иной аппаратуры для решения различных вопросов...

Хочется остановиться на возможности самостоятельного получения специалистами концентрированной информации в данной предметной области из целого ряда источников. В первую очередь это, конечно, специализированная литература. Ее обширный перечень дан в конце настоящей книги. В то же время авторы рекомендуют обратить особое внимание на следующие источники:

Хорее А. А. Способы и средства защиты информации.— М.: МО РФ, 1998. — 316с.

Лысов А. В.. Остапенко А. Н. Промышленный шпионаж В.России: методы и средства,— СПб.: Лаборатория ППШ, 1994.—71 с.

Ярочкин В. И. Технические каналы утечки информации.— М.:ИПКИР, 1994.— 106с.

Халяпин Д. Б., Ярочкин В. И. Основы защиты информации.— М.:ИПКИР, 1994.—125с.

Лысов А. В., Остапенко А. Н. Телефон и безопасность.— СПб, Лаборатория ППШ, 1995.— 105 с.

Вартанесян В. А. Радиоэлектронная разведка. — М.: Воениздат, 1991.— 254 с.

Интересные материалы можно найти в целом ряде периодических изданий, таких, как:

«Системы безопасности связи и телекоммуникаций» — издатель компания «Гротек», Москва;

«Защита информации. Конфидент» — издатель 000 «Конфидент», С.-Петербург;

«Специальная техника» — учредитель ОАО ХК «Электрозавод», Москва;

«Иностранная печать о техническом оснащении полиции зарубежных государств» — ежемесячный информационный бюллетень ВИНИТИ, Москва;

«Бизнес и безопасность»—издатель 000 «Шанс», Киев;

«Жизнь и безопасность» — ежеквартальный журнал, С.-Петербург;

«БДИ» (Безопасность, Достоверность, Информация), С.-Петербург;

«Оперативное прикрытие» — издатель 000 «Оперативное прикрытие», С.-Петербург и некоторые другие.

Перспективным направлением оперативного получения специальных сведений по рассматриваемой проблеме в настоящее время является и Интернет.

Остановимся на этом направлении более подробно, так как главная проблема в сети — найти нужную информацию. Для начала приведем несколько адресов, где собраны достаточно богатые и представительные коллекции ссылок на тему безопасности вообще.

Прежде всего, следует обратиться к одному из наиболее полных каталогов ресурсов российской части Интернета. Это «Рамблер» (или Rambler). Войдя в раздел «Безопасность» тематической части этого каталога (hyperlink http://counter-windows-1251.rambler.ru/top100/security/), можно подробно изучить более 200 ссылок на разные адреса. Надо, правда, иметь в виду, что часть ссылок отправит вас на различные разделы одних и тех же сайтов.

В течение 1998 года появилось несколько специализированных каталогов ресурсов российского Интернета, посвященных теме безопасности.

Наиболее «вместительным» из таких каталогов оказалась коллекция ссылок, собранная г-ном Свирским (hyperlink http://www.corbina.net/~ksi/). Все ссылки организованы в тематические разделы. Есть также ссылки на

некоторые зарубежные ресурсы. К сожалению, не все они «работают» из-за постоянно меняющейся, «живой» обстановки в Интернете. Это неизбежная беда большинства коллекций адресов.
Другой специализированный каталог ресурсов можно найти на сайте Санкт-Петербургской компании «Регионэксперт» (hyperlink http://www.regionexpert.ru/). Здесь также можно искать информацию о ресурсах по тематическим разделам. Почти все ссылки снабжены краткими комментариями. Не все из приведенных адресов имеют представительство в Интернете.
Тем, кого интересует Украина, пригодится сервер, поддерживаемый Киевским журналом «Бизнес и Безопасность» (hyperlink http://www.bsm.com.ua/). В разделах «Белые страницы» и «Желтые страницы» (которые почему-то выглядят совершенно одинаково) представлено большое количество украинских фирм, относящихся к заявленной тематике. К сожалению, пока лишь немногие компании на Украине имеют свое «Интернет-представительство».
Приведем некоторые, наиболее интересные адреса, где можно найти информацию, относящуюся к проблемам защиты информации и противодействию промышленному шпионажу.
Прежде всего надо назвать самый первый российский сервер, посвященный специально этой теме. Это Spy Market Pro (http:/www.spymarket.com/), принадлежащий Санкт-Петербургской компании «СмерШ Техникс» и созданный (при некотором участии Лаборатории ППШ) еще в начале 1997 года. На сервере немного собственно информации. Один из разделов содержит небольшое количество ссылок на российские компании (раздел платный — этим и объясняется малое количество ссылок). Есть две библиотеки: «старая» и «новая». Одним из наиболее интересных и посещаемых разделов сервера является его дискуссионная зона. Это одно из очень немногих мест русскоязычного Интернета, где «встречаются» специалисты и потребители товаров и услуг в области противодействия промышленному шпионажу.
«Территория взлома» — так называется сервер (hyperlink http://www.hackzone.ru/), содержащий несколько разделов, каждый из которых достоин отдельного повествования. Здесь можно найти статьи, периодические обзоры и вообще много интересной и полезной информации.
Следующий сервер зарегистрирован в Германии, но создан и поддерживается выходцами из России. Называется он «Werwolf» (hyperlink http://www.werwolf.de/). Здесь тоже много интересной и полезной информации по компьютерной безопасности (и не только). Очень рекомендуем посетить это место. Большую часть материалов можно читать на русском языке.
«Частная жизнь в Интернете» (hyperlink http://www.tamos.com/privacy/ru/). Этот сайт полезен всем, кого интересуют вопросы обеспечения собственной анонимности при работе в сети. Интересно и доступно изложены понятия о криптографии и стеганографии, о возможностях поиска людей по адресу и т. д. Множество полезных ссылок, которыми изобилуют тексты.
Различные документы по компьютерной безопасности выложены на личных страничках Казеннова Владимира Николаевича (hyperlink http://www.win.wplus.net/~kvn/compsec.htm)). Рекомендуем всем интересующимся.
На сервере питерского интернет-провайдера Web Plus есть интересный раздел (hyperlink http://wwwwin.support.wplus.net/security/index.htm), где изложены практические рекомендации по обеспечению сохранности паролей пользователей и безопасной конфигурации пользовательских компьютеров от посягательств злоумышленников. Очень рекомендую всем, кто обеспокоен проблемой создания надежной защиты своих кошельков от любителей пользоваться Интернетом за чужой счет.
Не только компьютерная безопасность, но также и другие проблемы

безопасности освещены в проекте «БИБ: Библиотека Информационной Безопасности» (hyperlink http://www.pps.ru/bib/index.html). Этот проект — наследник «старой» библиотеки на Spy Market Pro. К сожалению, работы по созданию БИБ'а затянулись, и остается надеяться, что они все же будут завершены.

«Радиошпион» (hyperlink http://www.chat.ru/~radiospy/) — это специализированный интернет-журнал, содержащий много материалов, относящихся к техническим каналам утечки информации. Правда, не совсем ясно, в каком направлении будет развиваться этот сайт. Пока же здесь, к сожалению, больше материалов, посвященных несанкционированному получению информации. Рекомендуется тем, кто хочет убедиться в ее доступности и незащищенности от посягательств злоумышленников.

«Конфидент. Защита информации» (hyperlink http://www.confident.ru/magazine/Page I /Page l.htm) — Интернет-вариант достаточно известного журнала. Рассматриваются в основном вопросы, посвященные компьютерной безопасности и противодействию промышленному шпионажу.

«БДИ» (Безопасность, Достоверность, Информация) — еще один журнал, где освещаются различные аспекты безопасности. Адрес: hyperlink http://www.bdi.spb.ru.

Московское издательство Groteck (http://www.groteck.msk.ru/) известно своими журналами и каталогами на темы безопасности, телекоммуникаций и др. На сайте издательства нет «Интернет-дубликатов» печатных версий. Но здесь есть еженедельные выпуски новостей, и это, видимо, единственное место в Интернете, где периодически публикуются новости по тематике «безопасность».

Только что родился совершенно новый сервер, называющийся «Все о радиомониторинге» (hyperlink http://radiomon.8m.com/). Это совместный проект Госсвязьнадзора и московской фирмы НЕЛК. Пока рано говорить, насколько будет удачен этот проект, но планы неплохие.

Фирма «АНКАД» (hyperlink http://www.microdin.ru/~ancud/index.html) предлагает криптоплаты, ПО к ним, смарт-карточные технологии и скремблеры для защиты телефонных разговоров.

«Центр информационной безопасности Маском» (hyperlink http://www.mascom.ru) — так называется одна из наиболее известных компаний в области технической безопасности. Особая специализация — телефонные каналы связи. Своя продукция: скремблеры серии SCR. Поставляют также различную продукцию российских и зарубежных производителей. Предлагают услуги по аттестации объектов, обучение.

«НПЦ Фирма НЕЛК» (hyperlink http://www.aha.ru/~nelk/) — еще одна известная компания. Специализируется на разработках программного обеспечения и программно-аппаратных комплексов радиомониторинга. Поставляют оборудование других производителей, оказывают услуги. Наиболее известные торговые марки собственных продуктов: Sedif, «Крона».

«Радиосервис» (hyperlink http://www.aha.ru/~rserv/) тоже специализируется на разработках программного обеспечения и программно-аппаратных комплексов для радиомониторинга. Узкая специализация позволяет сконцентрировать внимание специалистов-разработчиков на одной конкретной теме. Это дает свои плоды, поэтому продукты серии RS достаточно хорошо известны, как минимум, в России и ближнем зарубежье.

«Радиус ТСБ» (hyperlink http://www.aha.ru/~radius/) — одна из очень немногих торговых компаний, представленных в Интернете (конечно, на рынке безопасности). К сожалению, сервер «неживой»: обновления бывают крайне редко, нет возможности оформить заказ через Интернет и т. д. Для торговой компании это, как представляется, не очень правильный способ представить себя в Интернете. Красивая витрина.

Фирма «РелТех» (hyperlink http://www.reltech.ru/) занимается

разработкой и производством специальной аппаратуры для контроля за пейджинговыми сообщениями, переговорами в аналоговых стандартах сотовой связи и др. Вся спецтехника предназначена для субъектов ОРД, деятельность фирмы лицензирована ФСБ.

Теперь о сайтах компаний Санкт-Петербурга.

Фирма «Безопасность Бизнеса» (hyperlink http://www.secur.spb.ru/index.htm) предлагает разнообразную технику. Собственные разработки и производство: изделия марки «Барьер» для защиты телефонных линий. В соответствии с лицензиями ФСБ компания предлагает спецтехнику для субъектов ОРД. Интересный раздел сайга: «Страницы безопасности».

Фирма «Бэтмэн» на своем сайте (hyperlink http://www.batman.ru/) предлагает своеобразную выставку технических средств безопасности от различных производителей. Не рекомендуется смотреть этот сайт с помощью браузера от фирмы Netscape Communications. Видимо, есть ошибка в написании HTML-кода.

ЗАО «Лаборатория ППШ» (hyperlink http://www.pps.ru/) — еще одна ведущая питерская фирма. Из наиболее известных собственных разработок нужно назвать так называемые «подавители диктофонов». На сайге много информации о различных приборах и средствах как поиска, гак и защиты технических каналов утечки информации. Услуги: аттестация объектов, сертификация средств защиты, обследование помещений, консультации и обучение.

Особняком стоит сервер, целиком посвященный одному прибору — ST031 «Пиранья» (http://www.piranha.ru/), разработанному компанией «СмерШ Техникс». Прибор сам по себе достаточно интересен и в определенной степени уникален.

Сервер компании «СмерШ Техникс» (hyperlink http://www.spymarket.com/smerch). Компания занимается разработкой и производством собственных средств защиты информации. Сервер небольшой, но продукты интересные. К сожалению, не все они представлены на сайте. Поскольку «СмерШ Техникс» предпочитает реализовывать свою продукцию через дилеров, рекомендуем посмотреть их список. В ряде случаев у дилеров можно получить более подробную и развернутую информацию о продуктах этой компании.

Обязательно надо упомянуть о компании «Центр Речевых Технологий» (hyperlink http://www.stc.rus.net/). Это ведущая российская компания в области шумоочистки сигналов как в реальном времени, так и записанных на какие-либо носители.

Другие регионы России гораздо меньше представлены в Интернете. Как правило, представленные в Сети компании предлагают, кроме средств защиты информации, системы сигнализации, теленаблюдения, радиосвязи и др. Очень кратко перечислим некоторые из адресов. В большинстве случаев собственных разработок нет, предлагается оборудование других российских и зарубежных производителей.

В Архангельске — компания «КОНДОР-Техно» (hyperlink http://www.arh.ru/~condortn/)/.

Екатеринбург — компания «Центавр» (hyperlink http://www.skyman.ru/~centavr/)/.

Липецк — компания «Айра» (hyperlink http://aira.lipetsk.ru/)/.

Новосибирск — «Центр Информационной Безопасности» (hyperlink http://www.nsk. su/~security/)/.

Саратов — фирма «Коронэль» (hyperlink http://www.sarexpo.ru/koronel/).

Хабаровск — «Лотос Системы» (hyperlink http://lotos.khv.ru/).

## ПРИЛОЖЕНИЯ

## Приложение 1

**Рекомендации по оценке защищенности конфиденциальной информации от ее утечки за счет побочных электромагнитных излучений**

Если работа вашей фирмы связана с выполнением государственного заказа, то скорее всего вам не обойтись без получения лицензии на работу с государственной тайной, а следовательно, и проверки аппаратуры на наличие возможно внедренных «закладок» и на наличие и опасность технических каналов утечки информации (см. п. 2.2). Однако если такой необходимости нет, то в ряде случаев можно обойтись и своими силами, так как стоимость подобных работ все же достаточно высока.

Как уже отмечалось, одним из наиболее опасных технических каналов утечки конфиденциальной информации является наличие побочных электромагнитных излучений (ПЭМИ), возникающих при работе электронных устройств (факсимильных и телефонных аппаратов, мини-АТС, компьютеров, принтеров, модемов, сканеров и т. д.). Характер ПЭМИ определяется назначением, схемными решениями, элементной базой, мощностью устройства, а также конструкцией и материалами, из которых изготовлен его корпус. Излучение может происходить в довольно широком диапазоне частот (от единиц герц до единиц гигагерц), а дальность реального перехвата информации достигать сотен метров.

Для проведения полного объема работ по исследованию опасности ПЭМИ необходимо обладать:

>• парком дорогостоящей контрольно-измерительной аппаратуры с соответствующим метрологическим обеспечением;

>• высококвалифицированным персоналом;

>• специальными методиками проведения измерений и математическим аппаратом расчета результатов.

В то же время для защиты коммерческой информации задачу оценки опасности ПЭМИ можно решить ограниченными средствами. Для этого достаточно уметь задавать тестовый режим для проверяемой аппаратуры и иметь набор радиоприемных устройств (РПУ), работающих в диапазоне 0,01...1000 МГц. Желательно, чтобы РПУ обладали возможностью отключения системы автоматической регулировки усиления и функцией регулировки полосы пропускания.

Контроль может быть осуществлен как инструментальным способом, заключающимся в физической проверке невозможности перехвата ПЭМИ за пределами контролируемой территории, так и расчетно-инструментальным.

При проведении контроля любым из перечисленных способов тестовый режим должен задаваться путем формирования в проверяемой аппаратуре такого сигнала, который, с одной стороны, легко идентифицируется при приеме, а с другой — переводит аппаратуру в состояние, при котором уровень побочных излучений максимален.

Так, например, для элементов телефонных сетей (мини-АТС, факсимильные, телефонные аппараты и т. д.) это прохождение сигнала «занято» при поднятой трубке. Для систем внутреннего телевидения — передача миры (картинки, состоящей из чередующихся черно-белых полос). Для средств электронно-вычислительной техники (ЭВТ) — использование пачек импульсов с длительностью:

>• τи= 0,6 мкс — для проверки процессора;

>• τи = 0,25 мкс — для проверки гибкого магнитного диска;

>• τи = 0,05 мкс — для проверки жесткого магнитного диска;

**>•** τи = 0,06 мкс — для проверки монитора;

>• τи = 4 мкс — для проверки матричного печатающего устройства.
Наиболее просто контроль достаточности защиты коммерческой информации от утечки через ПЭМИ осуществляется инструментальным способом. При этом выполняется следующая последовательность операций.
1. Аппаратура контроля устанавливается в местах возможного расположения технических средств разведки.
2. Отключается система автоматической регулировки усиления РПУ.
3. Выставляется требуемое значение полосы пропускания приемного устройства (Δfп = 6 кГц — при контроле излучений оборудования телефонных сетей; Δfп = 15,6xM кГц, где М — число «белых» полос в мире; Δfп =1/τи, при контроле излучений средств ЭВТ, где τи — длительность импульса в пачке тестового сигнала).
4. Включается тестовой сигнал на проверяемой аппаратуре.
5. Осуществляется поиск излучения модулированного тестовым сигналом в диапазоне частот 0,01... 1000 МГц.
6. При его обнаружении принимается решение о необходимости проведения дополнительных мероприятий по защите информации.
Недостатком рассмотренного способа являются относительно высокие требования к пороговой чувствительности приемных устройств Uo (не хуже 1 мкВ) и наличию специальных комбинированных магнитных и электрических антенн, при которых обеспечивается Uo.
Если эти требования не выполняются либо отсутствует возможность проведения исследований на границе контролируемой территории (например, она приходится на офис соседней организации), то можно воспользоваться расчетно-измерительным способом, который заключается в проведении следующих операций.
1. Аппаратура контроля устанавливается на некотором расстояния Rк = 1 м от проверяемого устройства.
2. Включается тестовой сигнал.
3. Осуществляется поиск тестового сигнала аналогично тому, как это делалось 9 приведенной выше методике.
4. При обнаружении сигнала осуществляется измерение уровня сигнала в присутствии шумов Uс+ш на входе РПУ с помощью измерительной радиоконтрольной аппаратуры (см. п. 2.3.3).
5. Для всех частот, на которых были обнаружены излучения сигнала, измеренные значения Uс+ш заносятся в табл. П. 1.1.
6. Отключается контролируемая аппаратура и на всех частотах, на которых был обнаружен тестовый сигнал, измеряются уровни шумов Uш, которые также заносятся в табл. П. 1.1.

**Таблица П. 1.1. Результаты измерений и расчетов**

№ п/п /Частота сигнала/с, МГц /Уровень сигнала в присутствии шумов Uс+ш, мкВ /Уровень шума Uш, мкВ /Уровень сигнала Uс,мкВ

1 / // /

2 / / / /

Если чувствительность РПУ хуже, чем 10 мкВ, то для определения уровня Uш целесообразно воспользоваться аналитическим способом, в соответствии с которым:

Uш = ЕшxhД

где hд — действующая высота антенны, а Еш — шумовая напряженность электрического поля. Ориентировочные значения Еш для крупного промышленного города приведены в табл. П. 1.2.

**Таблица П.1.2. Ориентировочные значения Еш для крупного промышленного города**

f, МГц /0,1...1 /1...10 /10...100 /100...1000

Еш, мкВ/м /1...500 /0,8... 100 /0.1...10 /0.1...1

7. По формуле $U_c = \sqrt{U_{c+ш} - U_ш^2}$ рассчитываются значения уровня сигнала U на входе приемника контроля, которые также заносятся в табл. П. 1.1.
8. Расчетная дальности R , на которой возможен перехват ПЭМИ, находится из соотношения:

$$R_п = \frac{R_к \cdot U_c}{U_ш}.$$

9. Если расчетная величина R больше, чем радиус контролируемой зоны R , то необходимо учесть ослабление напряженности электромагнитного поля искусственными (или естественными) преградами.
С учетом ослабления электромагнитных волн возможная дальность перехвата ПЭМИ будет определяться значением:

$$R_{п_0} = \frac{R_к \cdot U_c}{\sqrt{K} \cdot U_ш},$$

где К — ослабление мощности сигнала преградой.
10. Если величина все же превышает радиус контролируемой зоны Rкз, то необходимо предпринять дополнительные меры по защите информации от перехвата.
Примечание.
Если аппаратура контроля не оснащена встроенными измерительными приборами, то уровни сигнала и шума на входе приемника контроля можно определить методом эквивалентного генератора, который заключается в следующем.
При обнаружении сигнала ПЭМИ радиоприемным устройством к его выходу подключается вольтметр и ручками усиления низкий и промежуточной частоты выставляется фиксированное значение выходного напряжения (система автоматической регулировки усиления при этом должна быть выключена).
Далее отключается антенна и на вход приемника подается сигнал с выхода генератора, настроенного на частоту РПУ (в режиме внутренней амплитудной модуляции с глубиной ma≈30 %).
Не меняя коэффициентов усиления приемного устройства, достигается выбранное фиксированное значение выходного сигнала за счет изменения уровня выходного напряжения генератора Uг
Эта процедура выполняется на всех частотах, на которых были обнаружены излучения контролируемой аппаратуры (табл. П. 1.1). Измерения делаются отдельно для сигнала в присутствии шумов (Uг≈Uс+ш) и шумов (Uг≈Uш).

## Приложение 2

**Выбор оптимальной структуры системы защиты информации**
Построение надежной и всеобъемлющей системы защиты информации вещь, несомненно, сложная и дорогая. Поэтому понятно желание руководителя любого ранга максимально надежно обеспечить конфиденциальность информации при минимальных затратах.
Естественно, что общая система защиты является достаточно разветвленной и включает в себя аутентификацию сотрудников, автоматическое разграничение их полномочий, защиту от несанкционированного доступа к информации (независимо от вида ее хранения), закрытие технических каналов утечки, а также ряд других элементов. Причем для каждого из этих элементов, как правило, необходимы свои технические средства защиты, в изобилии предлагаемые на российском рынке.

Таким образом, существует множество вариантов построения единой системы защиты конфиденциальной информации, отличающихся надежностью, быстродействием и ценой.
К сожалению, перечисленные факторы находятся во взаимном противоречии, и выбор конкретной комплексной системы защиты должен быть реализован на основе принципа «необходимой достаточности».
Применение этого принципа возможно только при наличии надежных показателей и критериев защищенности информации.
Этому требованию в полной мере отвечают оптимизирующие критерии, основанные на применении комплексных информационных показателей.
Методика их применения заключается в следующем:
I. Составляются различные варианты построения системы защиты, из которых необходимо выбрать одну наиболее предпочтительную.
II. Составляется список параметров, по которым сравниваются выбранные системы защиты.
В этот список, например, могут входить:
>• надежность системы;
>• быстродействие;
>• удобство ее прохождения зарегистрированными пользователями (ее прозрачность);
>• глобальность системы;
>• стоимость установки и поддержания.
Приведенный список может быть расширен в соответствии с задачами, возлагаемыми на систему защиты.
III. Устанавливается единая система оценки введенных параметров (например, 10-балльная). Показатель (оценка) должен быть тем выше, чем больше оцениваемый параметр отвечает интересам владельца системы защиты.
Так, например, чем выше надежность, тем параметр, ее оценивающий, ближе к 10, а чем выше цена, тем ближе к 1.
IV. Производится экспертная сравнительная оценка всех выбранных систем защиты по параметрам.
Пусть, например, имеется 4 системы защиты и каждой из них по каждому параметру выставляется оценка по 10-балльной системе.
Так, например, по параметру «I» (надежность) оценки могут быть расставлены следующим образом:
$I_{11}=3; I_{12}=1; I_{13}=8; I_{14}=10.$
Аналогично выставляются оценки по параметру «2» (быстродействие):
$I_{21}=1; I_{22}=6; I_{23}=3; I_{24}=5.$
по параметру «3» (прозрачность для зарегистрированного пользователя):
$I_{31}=9; I_{32}=8; I_{33}=2; I_{34}=6.$
по параметру «4» (глобальность системы):
$I_{41}=4; I_{42}=5; I_{43}=4; I_{44}=4.$
и по параметру «5» (стоимость):
$I_{51}=7; I_{52}=8; I_{53}=6; I_{54}=9.$
V. Полученные результаты заносятся в табл. П.2.1. Табл. П.2.1 анализируется по столбцам, и рассчитывается комплексный показатель защищенности для каждой из систем по формуле:

**Таблица 17.2.1. Оценка частных параметров сравниваемых систем**

| Номер оцениваемого параметра /Номер системы защиты /1 | /2 | /3 | /4 |
|---|---|---|---|
| 1 | /3 | /1 | /8 /10 |
| 2 | /1 | /6 | /3 /5 |
| 3 | /9 | /8 | /2 /6 |
| 4 | /4 | /5 | /4 /4 |
| 5 | /7 | /8 | /6 /9 |

$$I_{эj} = \sum_{i=1}^{n} ln \frac{I_{эj}}{I_{max}},$$ (1)

где j — порядковый номер системы защиты;
i — номер параметра, по которому производилась оценка;
n — количество оцениваемых параметров;
Iij— оценка i-го параметра для j-й системы защиты;
Imax— максимальное значение оценки параметра (для рассматриваемого примера Imax =10).
VI. Полученные результаты заносятся в табл. П.2.2.

**Таблица П.2.2. Комплексные показатели эффективности систем защити**

Номер систем защиты /1 /2 /3 /4

Значение комплексного показателя /-4,89 /-3,95 /-4?46А6 /-2,23

VII. В соответствии с критерием оптимизации

maxjIэj. (2)

Выбирается j-я система, имеющая максимальное значение показателя Iэj. Для рассматриваемого примера эта система защиты № 4.
Вместо энтропийного показателя (1) в предложенной методике может быть использован другой информационный показатель, обладающий аналогичными свойствами. Это показатель, основанный на методе наименьших квадратов:

$$I_{эj} = \sum_{i=1}^{n} \left[ I_{max} - I_{эj} \right]^2.$$ (3)

Таким образом, рассмотренная методика позволяет провести выбор оптимальной из имеющихся вариантов построения системы защиты на основе информационных показателей (1), (3) и критерия (2).

## Приложение 3

**Перечень предприятий и организаций, получивших лицензии на деятельность в области защиты информации**

№ п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки

1 /ЛГ0014, 000661 /№001 /30.05.95 /30.05.2001 /Специальный центр МЧС России (МЧС) /103012, Москва, Театральный проезд, 3,т.923-7894 /1;2;3;4;5;б /Продлено

2 /ЛГ0011, 000502 /№002 /30.05.95 /30.05.2001 /Научно-технический и сертификационный центр по комплексной защите информации «Атомзащитаинформ» (НТСЦ «Атомзащитаинформ») (Минатом России) /101000, Москва, а/я 911, т. 239-2262,239-4728 /1;2;3;4;5 /Продлено

3 /ЛГ 0019, 000943 /№003 /3.07.95 /03.07.2001 /АОЗТ «Российские наукоемкие технологии» (РНТ) /111141, Москва, 2-й проезд Перова поля, 9, т. 209-7677 /1.2; 2; 3,4; 5; 6 /Продлено и изменено

4 /ЛГ0017, 000849 /№004 /21.06.95 /21.06.2001 /ЦНИИатоминформ (Минатом России) /127434, Москва, Дмитровское ш., 2, т. 976-7272 /1.2;2;3;4;5а-в /Продлено и изменено

5 /ЛГ0008, 000393 /№ 005 /21.06.95 /21.06.2001 /5-й Центральный научно-исследовательский испытательный институт Министерства обороны Российской Федерации (5 ЦНИИ МО) (Минобороны России) /394052, Воронеж, ул. Краснознаменная, 153, т. (0732)56-1663 /1.2;2;3;4;5а-в, б /Продлено и изменено

6 /ЛГ0008, 000396 /№ 006 /09.08.95 /08.06.2001 /ОАО «Всероссийский научно-исследовательский институт автоматизации управления в непромышленной сфере» (ВНИИНС) /113149, Москва, ул., Сивашская, 4, корп.2, т.119-6842 /1.2;2.2;3;4;5а-в /Продлено и изменено

7 /ЛГ0011, 000507 /№007 /03.07.95 /03.07.2001 /ЗАО «Научно-производственная фирма «ПРОМТЕХН» (НПФ «ПРОМТЕХН») /121471, Москва, Можайское ш., 29/2, т. 166-7065 /1.2а-д; 2.2; 3; 4; 5а,б,в /Продлено

8 /ЛГ0011, 000509 /№009 /09.11.95 /09.11.98 /АОЗТ «Лаборатория новых информационных технологий «ЛАНИТ» /107066, Москва, ул. Доброслободская, 5, т.267-3038,261-5781 /1.2б,г,д,е; 2.2а-д; 36-е; 5; 6 /Срок действия истек

9 /ЛГ 0004, 000199 /№011 /16.11.98 /16.11.2001 /Федеральное государственное унитарное предприятие «Научно-производственное объединение прикладной механики им. академика М.Ф.Решетнева» (НПОПМ) (РКА) /662990, Железногорск Красноярского края, ул. Ленина, 52, т. (39197) 2-89-49, /1.2а-е;2;3а-е;4 /Продлено и изменено

Продолжение приложения 3

№ п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки

10 /ЛГ0011, 000512 /№012 /16.11.95 /16.11.2001 /Малое государственное внедренческое научно-производственное предприятие «Спектр» (МГВНПП «Спектр») (Минатом России) /117259, Москва, ул. Большая Черемушкинская, 25, т. 127-0482, 195-9496 /1.2а-в; 2; 3а-в; 4; 5а-в /Продлено

11 /ЛГ0011, 000513 /№013 /16.11.95 /16.11.98 /АООТ «НИЦЭВТ» (Минэкономики России) /113405, Москва, АО «НИЦЭВТ», т. 319-2745 /1.2а-в;2;3;4; 5а-в /Срок действия истек

12 /ЛГ 0004, 000189 /№014 /16.11.98 /16.11.2001 /ЗАО «НИЕНШАНЦ-ЗАЩИТА» /194175, Санкт-Петербург, Большой Сампсоньевский пр., 24,т. 542-9146, /3а-е;4 /Продлено с заменой бланка

13 /ЛГ0011, 000515 /№015 /16.11.95 /27.04.2000 /Калужский научно-исследовательский институт телемеханических устройств (НИИ ТУ) (Минэкономики России) /248650, Калуга, ул. Карла Маркса, 4, т. 4-35-00 /2;3.1-3.2а-б; 3.4-3.9а-б;4 /Продлено

14 /ЛГ0010, 000496 /№016 /30.01.97 /30.01.2000 /АООТ «Научно-производственное предприятие «Радуга» (НПП «РАДУГА») (Минэкономики России) /197342, Санкт-Петербург, ул. Кантемировская, 12, т. 542-3861,245-5142 /2.2; 3а-е;4 /Продлено и изменено

15 /ЛГ0011, 000517 /№017 /30.11.95 /30.11.2001 /Российский федеральный ядерный центр -Всероссийский научно-исследовательский институт технической физики (РФЯЦ-ВНИИТФ) (Минатом России) /456770, Снежинок Челябинской обл., ул. Васильева, 13, а/я 245, т. (35172) 3-25-40,3-22-42 /2; 3; 4; 5а-в /Продлено

16 /ЛГ 0003, 000101 /№018 /05.12.98 /05.12.2001 /Центр безопасности программного обеспечения и новых информационных технологий Ростовского ВИ РВ (Минобороны России) /344027, Ростов-на-Дону, пр. Октября, 24/50, т. (8632) 39-34-02, 31-31-33 /1.2; 2; 3; 4; 5а-в; 6 /Продлено с заменой бланка

17 /ЛГ0014, 000682 /№019 /18.04.96 /18.04.99 /Монтажно-технологическое управление «Икар» (Госкомсвязи России) /350033, Краснодар, ул. Ленина, 96,т.(861-2)-52-39-01 /1.2;2.1г-е; 2.2а-в; 3; 4; 5а-в /

18 /ЛГ0011, 000520 /№020 /05.12.95 /05.12.2001 /Физический институт им. П. Н. Лебедева (РАН) /117924, Москва, ГСП-1, Ленинский пр., 53, т. 135-4264,135-2430 /2; 3.4-3.9а-в; 4; /Продлено

19 /ЛГ0011, 000521 /№021 /05.12.95 /05.12.2001 /АОЗТ «СмерШ Техникс» /198148, Санкт-Петербург, а/я 732, т. (812) 560-4512 /3а, в, е /Продлено

20 /ЛГ0011, 000522 /№022 /05.12.95 /05.12,2001 /ТОО «Поликом» /143000, Одинцово Московской обл., б-р Л. Новоселовой, 5, т. 599-6572 /2; 3.3-3.9; 4; 5а-в /Продлено

21 /ЛГ0011, 000523 /№023 /18.12.95 /18.12.98 /Институт международного права и экономики (Минобразования России) /107066, Москва, ул. Энгельса, 3/5,стр.4,т.261-8045 /6 /Срок действия истек

Продолжение приложения 3

№ п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации). телефон /Виды деятельности /Особые отметки

22 /ЛГ0011, 000524 /№024 /18.12.95 /18.12.98 /АОЗТ «ПРОМСТРОНПРОЕКТ» /119827, ГСП, Москва, Г-48, Комсомольский пр., 42, т. 245-9475, 245-9481 /5 /Срок действия истек

23 /ЛГ0011, 000525 /№025 /18.12.95 /18.12.98 /Московский государственный инженерно-физический институт (технический университет), (Минобразования России) /115409, Москва, Каширское ш., 31, т. 324-3185, 324-3384 /1.2а-е;2;3а-е; 5а-в;6 /

24 /ЛГ0019, 000950 /№26 /27.10.97 /27.10.2000 /ГП «Московский институт теплотехники» (МИТ) (Минэкономики России) /127276, Москва, ул. Березовая аллея,10/1, т.907-1500 /1.2; 2; 3; 4; 5 /

25 /ЛГ0011, 000527 /№027 /26.12.95 /26.12.2001 /Координационный центр по созданию систем безопасности и управления «АТОМБЕЗОПАСНОСТЬ» (Минатом России) /141300, Московская обл. Сергиев Посад - 7, в/ч 51105, т. 584-9946 Л. /3.3-3.9а, б; 5а-в /Продлено

26 /ЛГ0011, 000528 /№028 /26.12.95 /26.12.98 /ООО "ПРОГРЕССТЕХ" /129128, Москва, проезд Кадомцева, 9, кв.17, т. 187-2465 /2; 3; 4; 5; 6 /Срок действия истек

27 /ЛГ0011, 000529 /№029 /28.12.95 /28.12.98 /ООО «РАДОНЕЖ» /109180, Москва, ул. Большая Полянка, 28, корп.1, т. 238-7256 /3.3-3.5а-ж; 3.8-3.9а-ж /Срок действия истек

28 /ЛГ0011, 000530 /№030 /28.12.95 /28.12.2001 /Военная инженерно-космическая академия имени А. Ф. Можайского (Минобороны России) /197082, Санкт-Петербург, П-82, ул. Ждановская, 13, т. (812) 235-8650, 235-8501 /2; 3.1; 3.4-3.9; 4; 5а-в;6 /Продлено

29 /ЛГ0011, 000531 /№031 /28.12.95 /28.12.98 /Войсковая часть 30895 (Минобороны России) /198903, Санкт-Петербург, Петродворец, ул.Разводная, 17, в/ч 30895, т. (812) 427-5079, 427-5372 /1.2;2;3;4 /Срок действия истек

30 /ЛГ0011, 000532 /№032 /28.12.95 /28.12.98 /АООТ «ЛОМО» (Минэкономики России) /194044, Санкт-Петербург, ул. Чугунная, 20, т. (812)248-5047,542-0396 /1.2а-в; 2; 3а-в; 4 /Срок действия истек

31 /ЛГ0011, 000533 /№033 /28.12.95 /28.12.98 /ООО «Олле-Сервис» /162002, Вологда, ул. Гагарина, 81, т. (817-22) 3-20-51 /2.1м; 3.3-3.5 /Срок действия истек

32 /ЛГ0011, 000534 /№034 /28.12.95 /28.12.98 /ООО «Научно-техническое агентство «АРТИ» /103009, Москва, ул. Грановского, 2, стр.1, пом.38, т. 291-9315, 291-3694 /1,2а, в-е; 2.2а-г; 3а,в-е /Срок действия истек

Продолжение приложения 3

№ п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки

33 /ЛГ0011, 000535 /№035 /28.12.95 /28.12.98 /000 «Охранное предприятие «АРГУС» /113149, Москва, ул. Сивашская, 4, корп. 2, т. 318-9611,318-9811 /2; 3.3-3.6а-е; 3.8-3.9а-е /Срок действия истек

34 /ЛГ0011, 000536 /№036 /17.01.96 /17.01.99 /АОЗТ «Большие и локальные информационные комплексы и системы» (БЛИКС) /101000, Москва, Большой Комсомольский пер.. 8/7, т. 262-0273 /3а, в-е;5 /

35 /ЛГ 0003, 000107 /№037 /17.01.99 /17.01.2002 /ОАО по проектированию предприятий транспортного машиностроения «ТРАНСМАШПРОЕКТ» /198005, Санкт-Петербург, Измайловский пр.,4, Т.(812)316-2992 /5 /Продлено с заменой бланка

36 /ЛГ0011, 000538 /№038 /17.01.96 /17.01.99 /Государственное научно-производственное объединение «Рубин» (Минэкономики России) /440630, Пенза, ул.6айдукова,1а, т. 62-41-04 /2а, в-е; 3; 4; 5а-в /

37 /ЛГ0011, 000539 /№039 /17.01.96 /17.01.99 /АООТ «Новосибирский завод химконцентратов» (Минатом России) /630038, Новосибирск, ул. Богдана Хмельницкого, 94, т. 74-09-13, 74-83-46 /2; 3.3-3.9а-в; /

38 /ЛГ0011, 000540 /№040 /17.01.96 /17.01.99 /ТОО «Специальное техническое бюро «БАГГЕР» (СТБ БАГГЕР) /107258, Москва, 1-я улица Бухвостова, 12/14, т. 962-6054, 963-9639 /4; 5а-в /

39 /ЛГ0011, 000541 /№041 /17.01.96 /17.01.99 /ТОО «Компания ПОИСК» /105215, Москва, ул.13-я Парковая, 27,т,463-5629 /2е; 3.3-3.9а-в /

40 /ЛГ0011, 000542 /№042 /18.01.96 /18.01.99 /Главный научно-исследовательский вычислительный центр Федеральной налоговой службы России (ГНИВЦ ФНС России) /103381, Москва, ул. Неглинная, 23,т.235-8754 /3г-е /

41 /ЛГ0011, 000543 /№043 /18.01.96 /18.01.99 /17-й Центральный проектный институт связи Министерства обороны (17 ЦПИС МО) (Минобороны России) /107014, Москва, Б-14, ул. Большая Оленья, 15а, т.168-1233 /3а-в;4;5 /

42 /ЛГ0011, 000544 /№044 /18.01.96 /18.01.2002 /НИИ специальной техники (НИИСТ) (МВД России) /101000, Москва, ул. Малая Лубянка, 16/4, т. 273-47029 /1.2а-в;2б-е;3а-в; 4; 56, в /Продлено

43 /ЛГ0011, 000545 /№045 /18.01.96 /18.01.99 /ТОО «Русский сезон» /236040, Калининград, Советский пр., 12, корп. 912, т. 21-70-61,22-64-07 /2.2; 3.4-3.6а; 4 /

44 /ЛГ0011, 000546 /№046 /22.01.96 /22.01.99 /АООТ «Московский научно-исследовательский институт радиосвязи» /109029, Москва, ул. Нижегородская, 32, т.272-5005,912-7878 /2а,б,д,е;4 /

Продолжение приложения 3

№. п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки

45 /ЛГ0011, 000547 /№047 /22.01.96 /22.01.99 /ТОО «Малое внедренческое предприятие «ТАЛИСМАН» /125083, Москва, ул. 8-е Марта, 10-12, т. 212-4283, 212-0662 /2г-е; 3а /

46 /ЛГ0011, 000548 /№048 /22.01.96 /22.01.99 /ТОО «Научно-производственное предприятие «ГЕРО ЛТД» /344007, Ростов-на-Дону, ул. Пушкинская, 70, т. 66-2306, 69-62-37 /2.2а-в; 3а-б; 3г-д /

47 /ЛГ0011, 000549 /№049 /22.01.96 /22.01.99 /000 «Торговый дом Александр и К» /344008, Ростов-на-Дону, ул. Большая Садовая, 37/39, т. 32-77-61 /2.2а-в; 3а-б; 3г-д /

48 /ЛГ 0008, 000400 /№50 /17.06.98 /17.06.2001 /ЗАО «АЛАДДИН Р.Д.» /101000, Москва, Милютинский пер., 14, т. 923-0588, 928-6066 /3.1г-е;3.2-3.9а-е /

49 /ЛГ0012, 000551 /№051 /26.05.95 /26.05.2001 /Производственное объединение «Северное машиностроительное предприятие» (ПО «Севмашпредприятие») (Минэкономики России) /164500, Северодвинск, Архангельское ш., 58, т. 9-4601 /2; 3 а-в; 3.4-3.7 г; 3.9г-е; 5в-в /Продлено

50 /ЛГ0004, 000162 /№052 /26.05.95 /04,09.2001 /«Московский региональный аналитический центр» (МРАЦ) (Правительство Москвы) /129010, Москва, пр. Мира, 48, стр. 3,т.280-6109 /1.2;2а,б,г-е;3; 4; 5а-в /Продлено и изменено

51 /ЛГ0012, 000553 /№053 /26.05.95 /26.05.2001 /АОЗТ «Защита информации» /117192, Москва, Ломоносовский пр., 31, корп. 2, т. 143-1293 /2; 3; 4; 5д, е /Продлено

52 /ЛГ0012, 000554 /№054 /26.05.95 /26.05.2001 /АОЗТ «Лаборатория противодействия промышленному шпионажу» (Лаборатория ППШ) /190000,Санкт-Петербург, пер.Гривцова, 1/64, т. 219-1137, 314-2259 /2,3; 4; 5; 6; 1.2 /Продлено

53 /ЛГ0019, 000947 /№055 /07.10.97 /07.10.2000 /ТОО «Фирма «ИнфоКрипт» ЛТД» /117571, Москва, пр. Вернадского, 86, корп.0,т.111-9240 /3.1г-е;3.7г-е; 3.2-3.6а-е; 3.8-3.9а-е /Продлено и изменено

54 /ЛГ0012, 000556 /№056 /02.06.95 /27.8.2001 /АОЗТ «Особое конструкторское бюро САПР» (ОКБ САПР) /113114, Москва, 2-й Кожевнический пер., 4/6, т. 235-1606,235-2990 /2;3 /Продлено и изменено

55 /ЛГ0019, 000929 /№057 /10.09.97 /10.09.2000 /АОЗТ «Многопрофильное внедренческое предприятие «СВЕМЕЛ» (МВП «СВЕМЕЛ») /125438, Москва, 4-й Лихачевский пер., 15, т.154-0201, 156-7187 /1.2а-е;2;3а-е;4; 5а-в /Продлено и изменено

56 /ЛГ0012, 000558 /№058 /15.06.95 /15.06.2001 /ТОО «Кировский региональный центр деловой информации» (КРЦДИ) /610005, Киров, ул. Мопра, 113, т. (8332) 65-3483,65-1936 /2.2; 3в-е; 4; 5а, б, в /Продлено

57 /ЛГ0001, 000013 /№059 /20.11.97 /20.11.2000 /ЗАО «Научно-техническая фирма «КРИПТОН» НИИАА» (Минэкономики России) /117420, Москва, ул. Профсоюзная, 78, т. 330-6283 /1.2а-е; 2; 3а-е; 4; 5а-в /Продлено и изменено

Продолжение приложения 3

№ п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки

58 /ЛГ0012, 000560 /№060 /20.06.95 /20.06.2001 /ЗАО «Щит» /141205, Пушкино Московской обл., Ярославское ш., д. 4-227,т.973-1044 /3а, б, в; 5а, 6в /Продлено

59 /ЛГ0012, 000561 /№061 /20.06.95 /20.06.2001 /Государственный научно-исследовательский институт радио (ГНИИ радио) (Госкомсвязи России) /103064, Москва, ул. Казакова, 16, т. 261-3694 /1.2а-е;3а-в;4 /Продлено

60 /ЛГ0012, 000562 /№062 /20.06.95 /20.06.2001 /ОАО «НОВО» /127434, Москва, ул. Дубки, 6, т. 210-2760, 210-2780 /1.2а-д;2а-е; 3.1-3.6а-ж;4;6 /Продлено

61 /ЛГ0012, 000563 /№063 /20.06.95 /20.06.98 /АОЗТ «Межрегиональное производственное объединение «Конус» (МПО «КОНУС») /113114, Москва, • 1-й Кожевнический пер., 5/1, т.235-3507,235-6834 /2а, б, д, е; 3.3-3.6а-е; 3.8-3.9 а-е; 4; 5а-в /Срок действия истек

62 /ЛГ0012, 000564 /№ 064 /26.06.95 /26.06.2001 /«Конструкторское бюро «Корунд-М» научно-исследовательского института системных исследований» (КБ «КОРУНД-М») (РАН) /109280, Москва, ул. Автозаводская,23, т. 274-6347, 277-2710 /36; 4 /Продлено

63 /ЛГ0012, 000565 /№065 /22.06.95 /22.06.98 /Научно-производственное объединение «Марс» (НПО «МАРС») (Минэкономики России) /432022, Ульяновск, ул. Солнечная, д 1, т. (8-842-2) 29-78-78 /2; 3а-е;4 /Срок действия истек

64 /ЛГ0012, 000566 /№066 /28.06.95 /28.06.98 /Центральный научно-исследовательский институт «АСУАГРОСЕРВИС» (ЦНИИ «АСУАГРОСЕРВИС») (Минсельхозпрод России) /103001, Москва, ул. Большая Садовая, 2/46, т. 254-8647, 254-8929 /2е; 3.4а-е /Срок действия истек

65 /ЛГ0019, 000911 /№067 /22.07.97 /22.07.2000 /ОАО «ГИПРОСВЯЗЬ» /123833, Москва, ул. 3-я Хорошевская, 11, т. 197-1084, 197-1231 /5 /Продлено и изменено

66 /ЛГ0012, 000568 /№068 /28.06.95 /28.06.98 /АОЗТ «Центр новых компьютерных технологий» (ЦНКТ) /127018, Москва, ул. Образцова, 38, т. 289-2222, 289-3296 /2.2а-е; 3.1-3.6а-ж;4;б /Срок действия истек

67 /ЛГ0012, 000569 /№069 /28.06.95 /28.06.2001 /Центр комплексной безопасности информации государственного унитарного предприятия СНПО «Элерон» (ЦКБИ ГУП СНПО «ЭЛЕРОН») (Минатом России) /127018, Москва, ул. Генерала Белова, 14, т. 399-9637, 399-9904 /1.2а-в;2;3;4;.5 /Продлено

68 /ЛГ0012, 000570 /№070 /28.06.95 /28.06.98 /Центральный научно-исследовательский институт экономики, информатики, систем управления (ЦНИИЭИСУ) (Минэкономики России) /103104, Москва, Тверской б-р, 7/2, т. 291-8714,290-6017 /2;3.1а-е;3.2а-е; 3.9а-е; 4 /Срок действия истек

Продолжение приложения 3

№ /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки

69 /ЛГ0012, 000571 /№071 /28.06.95 /31.12.99 /Московский научно-исследовательский институт приборной автоматики (МНИИ ПА) (Минэкономики России) /111250. Москва, Красноказарменный проезд, 14а, т. 362-6562,361-5588 /2;3.1а-г;3.2а-б; 3.6а-в; 4; 5а-б /Продлено

70 /ЛГ0017, 000818 /№072 /28.06.95 /28.06.2001 /Государственный центральный институт повышения квалификации руководящих работников и специалистов (ГЦИПК) (Минатом России) /249020, Обнинск Калужской обл., ул. Курчатова, 21, т. (08439) 4-88-33 /1.2а-в;2;3а;4;6 /Продлено и изменено

71 /ЛГ0001, 000007 /№073 /28.06.95 /28.06.2001 /ГП «Испытательный центр сертификации и аттестации «Безопасные информационные технологии» (ИЦСА БИНТЕХ) (Гостехкомиссия России) /394036, Воронеж, ул. Студенческая, 36, т. 56-16-63 /1.1 г-ж; 1.2; 2; 3.1-3.2; 3.4-3.6; 3.8-3.9; 4; 5а-в /Продлено

72 /ЛГ 0003, 000108 /№073 (копия) /28.06.95 /28.06.2001 /Волгоградский филиал государственного предприятия «Испытательный центр сертификации и аттестации «Безопасные информационные технологии» (ИЦСА БИНТЕХ) (Гостехкомиссия России) /400001, Волгоград, ул. Рабочекрестьянская, 4, т.44-01-90 /1.1r-ж; 1.2; 2; 3.1-3.2; 3.4-3.6; 3.8-3.9; 4; 5а-в /Продлено

73 /ЛГ0017, 000806 /№73 (копия) /22.06.98 /22.06.2001 /Филиал ГП ИЦСА «БИНТЕХ» — «федеральное агентство информационной безопасности» (ФАИБ) (Гостехкомиссия России) /141260, Московская обл., Красноармейск, ул. Центральная, 17, т. 263-3058, 263-3643 /1.2, 1.1г-ж;2; 3.1-3.2; 3.4-3.6; 3.8-3.9; 4; 5а-в; /Продлено

74 /ЛГ0017, 000841 /№074 /26.06.98 /26.06.2001 /ТОО «Частное охранное предприятие «Троян» (ЧОП «ТРОЯН») /123098, Москва, ул. Живописная, 50, т. 190-2527 /3.1г-с;3.2-3.9а-с /Продлено и изменено

75 /ЛГ0017, 000817 /№075 /28.06.95 /28.06.2001 /ТОО «Внедренческая

холдинговая фирма «Александр» (Фирма «АЛЕКСАНДР») /129110, Москва, ул. Средняя Переяславская,27,стр.1, т.281-0225 /2; 3а-е; 4 /Продлено и изменено

76 /ЛГ0012, 000576 /№076 /30.06.95 /30.06.2001 /Государственное научно-производственное предприятие «ИНФОРМАКУСТИКА» (ГНПП «ИНФОРМАКУСТИКА») (Минэкономики России) /197136, Санкт-Петербург, Чкаловский пр., 50, т.346-4498,238-6489 /2; 3а-в;4 /Продлено

77 /ЛГ0019, 000931 /№077 /12.09.97 /12.09.2000 /АОЗТ «Научно-технический центр «Критические информационные технологии» (НТЦ «КИТ») /190031, Санкт-Петербург, ул. Гастелло, 15, Т.(812)291-7924 /1.2; 2; 3; 4; 5а-в /Продлено и изменено

78 /ЛГ0012, 000578 /№078 /04.07.95 /04.07.98 /ЗАО «СИГНАЛ-КОМ» /125315, Москва, ул. Усиевича, 19,т. 155-5496, 152-8555 /1.2а,г,д,е; 2.2 а-г, 3.1-3.9а,в-с /Срок действия истек

79 /ЛГ0017. 000827 /№079 /04.07.95 /04.07.2001 /ТОО «Научно-производственная фирма «КРИСТАЛЛ» (НПФ «КРИСТАЛЛ») /440017, Пенза, ул. Красная, 40, т. (841-2) 46-27-00 /1,2г-е; 3г-е; 5а, б /Продлено и изменено

Продолжение приложения 3

№ п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки

80 /ЛГ0012, 000580 /№080 /25.07.95 /25.07.98 /ТОО «Научно-производственный центр «ДИВЕКОН» (НПЦ «ДИВЕКОН») /115580, Москва, ул. Мусы Джалиля, 5, корп.5, кв.1017, т. 465-0220 /2;3.1а-в;3.3- -3.9а-в; 5д, е /

81 /ЛГ0012, 000581 /№081 /25.07.95 /25.07.98 /Ассоциация защиты информации «Конфидент» /193060, Санкт-Петербург, ул. Пролетарской диктатуры, 2,  Смольный, т. 278-1392, 568-1035 /3.1-3.3в-е;3.4г-е; 3.6г-е; 3.9г-е /Срок действия лицензии истек

82 /ЛГ0017, 000804 /№082 /25.07.95 /25.07.2001 /Федеральное государственное унитарное предприятие «Научно-производственное предприятие «Гамма» (ФГУП «НПП «Гамма») /117420, Москва, ул. Профсоюзная, 78, т. 128-6993,330-3388 /1.2;2;3;4;5а-в /Продлено и изменено

83 /ЛГ0017, 000805 /№082 (копия) /25.07.95 /25.07.2001 /ЗАО «Центр защиты информации «Гамма», — дочернее предприятие НПГП «Гамма» (Минэкономики России) /117513, Москва, Ленинский пр., 117,т. 330-5333 /1.2;2;3;4;5а-в /Продлено

84 /ЛГ0012, 000583 /№ 083 /25.07.95 /25.07.2001 /Межотраслевой специальный учебный центр (Минатом России) /249020. Калужская обл., Обнинск, ОС-7, а/я 120, т. (08439) 4-85-10,4-82-22 /2а-е; 3.4а, б, г 3.5а, б; 3.6а, б, г; 3.7а;3.8а,б; 3.9а, б, г; 4; 6 /Продлено

85 /ЛГ0012, 000584 /Х" 084 /25.07.95 /25.07.2001 /Научно-исследовательский институт «Восход» (НИИ «ВОСХОД») (Госкомсвязи России) /117607, Москва, ул. Удальцова, 85, т. 931-7700, 931-9225 /1.2;2;3.1а-е 3.4-3.9а-е; 4; 5а-в /Продлено

86 /ЛГ 0008, 000380 /№085 /21.04.98 /21.04.2001 /Пензенский филиал государственного унитарного предприятия научно-технического центра «Атлас» (ПФ НТЦ «АТЛАС») (ФАПСИ) /440601, Пенза, ул. Советская, 9, т. (8412) 66-39-06 /1.2а-е;2;3а-е;4; 5а-в /Продлено и изменено

87 /ЛГ0012, 000586 /№ 086 /25.07.95 /25.07.2001 /АООТ Научно-исследовательский испытательный центр систем управления «ЭКОР» (НИИЦСУ «ЭКОР») (Минэкономики России) /109147, Москва, ул. Большая Андроньевская, 23, т. 270-0201, 270-0172 /2; 3а-е; 4; 5а-в /Продлено

88 /ЛГ 0004, 000167 /№ 087 /26.07.95 /22.9.2001 /ЗАО «Кобра» /600001, Владимир, ул. Студеная гора, 3, т.(09222) 29-11-90,29-83-56 /2; 3а-е;4 /Продлено и изменено

89 /ЛГ0012, 000588 /№088 /26.07.95 /26.07.98 /АОЗТ «КОБРА ЛАИН» /191028, Санкт-Петербург, ул. Салтыкова-Щедрина, 22, пом, 3-Н, т. (812) 272-7465 /3.1-3.4г;3.6г; 3.9г /Срок действия истек

90 /ЛГ 0019, 000913 /№089 /22.07.97 /22.07.2000 /АООТ «Научно-исследовательский институт молекулярной электроники и завод «Микрон» (НИИ «Микрон») (Минэкономики России) /103460, Москва, Зеленоград, АООТ НИИМЭ и завод «Микрон», т. 536-8217,535-1589 /1.2;2;3;4 /Продлено и изменено

Продолжение приложения 3

№ п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки

91 /ЛГ0012, 000590 /№090 /26.07.95 /26.07.2001 /Центральный научно-исследовательский институт «Центр» (ЦНИИ «Центр») (Минэкономики России) /123231, Москва, ул. Садовая Кудринская, 11/13, т. 252-5574 /2; 3.4-3.6а; 3.9а; 4 /Продлено

92 /ЛГ0017, 000839 /№091 /26.07.95 /26.07.2001 /Федеральное государственное предприятие «Научно-исследовательский институт точных приборов» (НИИ «ТОЧПРИБОР») (Минэкономики России) /127490, Москва, Юрловский проезд, 1,т. 181-4518, 181-0370 /2; 3.4-3.9а-в;4 /Продлено и изменено

93 /ЛГ0012, 000592 /№092 /26.07.95 /26.07.98 /Государственный специализированный проектный институт (ГСПИ) (Минатом России) /107014, Москва, Новорязанская ул., 8а, т.265-8285,267-3335 /5 /Срок действия истек

94 /ЛГ0012, 000593 /№093 /26.07.95 /26.07.98 /Государственный центральный научно-исследовательский радиотехнический институт (ГосЦНИРТИ) (Минэкономики России) /107066, Москва, ул. Новая Басманная, 20у т.267-4393,267-1559 /2; 3.1а; 3.4-3.6а; 3.9а; 4 /Документы на рассмотрении

95 /ЛГ 0004, 000179 /№094 /26.11.97 /26.11.2000 /000 «Центр безопасности информации «МАСКОМ» /117571, Москва, пр. Вернадского, 86,корп.0, ком. 119,т.437-4194 /2; 3а-е; 4; 5а-в; 6 /

96 /ЛГ0001, 000004 /№95 /03.11.97 /03.11.2000 /ЗАО «ТЕЛЕФОРМ» /107078, Москва, Скорняжный пер., 1, т. 246-8842 /3в-ж /

97 /ЛГ0012, 000596 /№096 /09.08.95 /09.08.98 /Российский научно-производственный центр геоинформации «РОСГЕОИНФОРМ» (Роскартография) /115230, Москва, Варшавское ш., 42, т. 111-1221 /1.2; 2; 3; 4; 5а-в /Срок действия истек

98 /ЛГ0017, 000846 /№097 /09.08.95 /09.08.2001 /ОАО «Сатурн» /107553, Москва, ул. Большая Черкизовская, 103/105, т. 161-1210 /2; 3а-в; 4;5 /Продлено и изменено

99 /ЛГ0001, 000047 /№099 /09.02.98 /09.02.2001 /Военная академия связи им. С. М. Буденного (ВАС) (Минобороны России) /194064, Санкт-Петербург, Тихорецкий пр., д 3, Т.(812)556-9315 /2; 4; 6 /Продлено и изменено

100 /ЛГ0008, 000369 /№ 100 /06.04.98 /06.04.2001 /Научно-исследовательский центр информатики при МИД России (НИЦИ МИД) (МИД России) /119021, Москва, ул. Остоженка, 53/2, т. 203-1802,246-7945 /2а, г-с; 3.4-3.9а-д;4 /Продлено и изменено

101 /ЛГ0013, 000601 /№ 101 /10.08.95 /10.08.98 /ТОО «Фирма «ЛЕКС» /117454, Москва, ул. Лобачевского, 66-а, т.917-4845 /2. 1е; /Срок

действия истек
102 /ЛГ0013, 000602 /№ 102 /16.08.95 /16.08.2001 /Войсковая часть 01168 (Минобороны России) /123007, Москва, 1-й Хорошевский проезд, f, т.945-7175 /1.2г-ж;2а; 3.1-3.4г-ж; 3.7г-ж; 3.9г-ж, 4 /Продлено
Продолжение приложения 3
№ п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки
103 /ЛГ0013, 000603 /№103 /16.08.95 /16.08.98 /АОЗТ «ЭДВАНС» /107392, Москва, ул. Просторная, 14, корп. 1, т. 925-4909 /1.2а-в;2а-е; 3а-ж; 4; 5 /Срок действия истек
104 /ЛГ0013, 000604 /№104 /16.08.95 /16.08.2001 /Научно-исследовательский институт «Квант» (НИИ «Квант») (Минэкономики России) /125438, Москва, 4-й Лихачевский пер., 15, т.156-7348,154-8021 /1.2а-е;2а-д;3;4; 5а-в /Продлено
105 /ЛГ0004, 000166 /№ 105. /16.08.95 /22.09.2001 /Войсковая часть 11135 (Минобороны России) /Москва, К-160, в/ч 11135, т. 302-9405,456-4383 /1.2; 2; 3; 4; 5а-в /Продлено и изменено
106 /ЛГ0004, 000178 /№106 /16.08.98 /16.08.2001 /ЗАО «Научно-производственный центр» Фирма «НЕЛК» /129110, Москва, Олимпийский пр., 22, т. 324-0125 /1.2г-е;2;3а-е /
107 /ЛГ0013, 000607 /№107 /25.08.95 /25.08.98 /Государственное испытательно-коммерческое предприятие «Ритм» (Минэкономики России) /101000, Москва, ул. Маросейка, 12, т. 206-9541 /2а, б, г, д, е; 3а-е; 4; 5а-в; 6 /Срок действия истек
108 /ЛГ0013, 000608 /№108 /16.08.95 /16.08.98 /АОЗТ «Производственно-коммерческое акционерное общество «А.Т.К.» /123459, Москва, б-р Яна Райниса, 6-1-123, т.459-4781,459-3791 /2.2а,б,д,е; 3.1-3.3а,в,д, е3.5-3.6а, в, д, е /Срок действия истек
109 /ЛГ 0008, 000363 /№109 /17.03.98 /17.03.2001 /ЗАО «СПЕЦЭЛЕКТРОНИКА» /150048, Ярославль, Московский пр.,153, т. (0852) 44-37-08,44-52-09 /1.2б;2а-д;3.1а-е; 3.3-3.9а-е;4 /Продлено и изменено
110 /ЛГ0013, 000610 /№110 /25.08.95 /25.08.2001 /Войсковая часть 64829 (ФСБ России) /101000, Москва, в/ч 64829, т. 224-8441,924-6118 /1.2; 2,3; 4; 5 /Продлено
111 /ЛГ0013, 000611 /№111 /25.08.95 /25.08.98 /АОЗТ «Застава» /193230, Санкт-Петербург, Искровский пр., 21, кв.280, Т.(812)350-6616 /1.2; 2,3; 4; 5; 6 /Срок действия истек
112 /ЛГ0013, 000612 /№ 112 /25.08.95 /14.04.98 /Научно-исследовательский институт средств вычислительной техники (НИИ СВТ) (Минэкономики России) /610602, Киров, НИИ СВТ, т. 67-95-38, 67-99-75 /2.2; 36; 4; 5а, б, в /Срок действия истек
113 /ЛГ0013, 000613 /№113 /25.08.95 /25.08.2001 /Всероссийский проектный и научно-исследовательский институт комплексной энергетической технологии (ВНИПИЭТ) (Минатом России) /197183, Санкт-Петербург, ул. Савушкина, 82, т. (812) 430-4571,430-0134 /2; 3.4а-в; 3;5а-в; 3.6а-в;4;5 /Продлено
114 /ЛГ0013, 000614 /№114 /1.09.95 /01.09.2001 /Российский центр «Безопасность» (РЦБ) (Минэкономики России) /129626, Москва, пр. Мира, 102, т. 287-0369 /1.2; 2; 3:4; 5а-в; 6 /Продлено
Продолжение приложения 3
№ п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки

115 /ЛГ0013, 000615 /№ 115 /15.09.95 /15.09.2001 /Научно-технический и сертификационный центр «Заслон» (НТСЦ «Заслон») (Минэкономики России) /125833, Москва, Миусская пл., 3, т. 972-7311, 251-0823 /1.2а-в;2;3а-в;4 /Продлено

116 /ЛГ0013, 000616 /№ 116 /15.09.95 /14.04.2001 /Государственный космический научно-производственный центр им. М. В. Хруничева (Минэкономики России) /121309, Москва, ул. Новозаводская,18, т. 145-8323,145-8036 /2.2; 3а-е; 4 /Продлено

117 /ЛГ0013, 000617 /№ 117 /15.09.95 /15.09.2001 /ООО «Центр безопасности информации» (ЦБИ) /141080, Московская обл., Юбилейный, ул. Тихонравова, 34, 4 ЦНИИ МО РФ, т. 515-1598 /1.2; 2; 3.1; 3.3-3.7; 3.9; 4; 5а-б, 6 /Продлено

118 /ЛГ0013, 000618 /№ 118 /09.11.95 /09.11.2001 /Войсковая часть 25714 (Минобороны России) /305542, Курск-42, ул. Блинова, 23, т. (071)302-35, /3.1-3.6а-е;3.9а-е; 4 /Продлено

119 /ЛГ 0004, 000187 /№ 119 /09.11.95 /09.11.2001 /ЗАО «Научно-инженерное предприятие «Информзащита» /127018, Москва, а/я 55, т. 289-4232 /2а-г; 3а-ж; 5а-в /Продлено с заменой бланка

120 /ЛГ0013, 000620 /№ 120 /15.09.95 /15.09.98 /ТОО «Септима Лтд» /129226, Москва, ул. Докукина, 4, т.923-0723, 925-3305 /1.2;2;Э;4;5а-в /Срок действия истек

121 /ЛГ0013, 000621 /№ 121 /15.09.95 /15.09.98 /Научно-исследовательский институт радиовещательного приема и акустики им. А .С. Попова (НИИРВПА) (Минэкономики России) /197376, Санкт-Петербург, наб.р.Крестовки,3, т.(812)234-4528,234-2945 /2; 3.9а-е;4 /Срок действия истек

122 /ЛГ0013, 000622 /№ 122 /15.09.95 /15.09.2001 /Государственное научно-производственное предприятие «Исток» (ГНПП «Исток») (Минэкономики России) /141120, Московская обл., Фрязино,ул. Вокзальная, 2а, т. 465-8611,465-8666 /2; 3а-в;4 /Продлено

123 /ЛГ0013, 000623 /№ 123 /25.09.95 /25.09.98 /Государственный научно-исследовательский институт моделирования и интеллектуализации сложных систем (ГНИИМИСС) /197376, Санкт-Петербург, ул. Профессора Попова, 5, т. (812)234-0415,234-9094 /2; 3; 4; 6 /Срок действия истек

124 /ЛГ0013, 000624 /№ 124 /25.09.95 /25.09.98 /Войсковая часть 96010 (Гостехкомиссия России) /103175, Москва, К-175, ул. Старая Басманная, 17, т.296-6498,293-0177 /1.2а;2; 3.3-3.8а-г; 4 /?

125 /ЛГ0013, 000625 /№ 125 /25.09.95 /25.09.2001 /Центральный физико-технический институт Министерства обороны Российской Федерации (ЦФТИ МО) (Минобороны России) /141300, Московская обл., Сергиев Посад-7, т. 584-9997, 584-9942 /1.2;2;3;4; 5а-в /Продлено

126 /ЛГ0013, 000626 /№ 126 /25.09.95 /25.09.98 /АОЗТ «Северо-Западный центр «Информационная безопасность» /196066, Санкт-Петербург, пр. Римского-Корсакова, 65/11, кв.31, т. (812)278-5884,114-0179 /2;3;4 /Срок действия истек |

Продолжение приложения 3

№ п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки

127 /ЛГ 0004, 000156 /№ 127 /29.09.95 /01.09.2001 /ЗАО «Анна» /111396, Москва, Союзный пр., 4, т. 301-7922, 301-7822 /3а-д /Продлено и изменено

128 /ЛГ0013, 000628 /№ 128 /03.10.95 /14.04.98 /Центральный НИИ «Гранит» (Минэкономики России) /191014, Санкт-Петербург, ул.

Госпитальная,3, т.271-4593,278-9803 /2; 4 /Срок действия истек

129 /ЛГ0013, 000629 /№ 129 /04.10.95 /04.10.2001 /АОЗТ «Научно-производственная фирма «Арго» (НПФ «АРГО») /414056, Астрахань, пер. Смоляной, 2, Т.(8512)25-30-61 /1.2;2;3;4;5а-в /Продлено

130 /ЛГ0013, 000630 /№ 130 /04.10.95 /26.04.2000 /Войсковая часть 60130 (Минобороны России) /199155, Санкт-Петербург, ул. Одоевского, 26, т. 350-4917, 350-6427 /2.2,3.16; 3.4-3.6а, б; 4 /Продлено

131 /ЛГ0013, 000631 /№131 /12.10.95 /12.10.98 /ТОО «Учебно-педагогический центр «Машиностроение (УПЦ «Машиностроение») /107005, Москва, ул. 2-я Бауманская, 5, т. 263-6792, 263-6794 /1.2; 2.2;?; 4; 5а-в; 6 /Срок действия истек

132 /ЛГ0013, 000632 /№ 132 /12.10.95 /12.10.98 /АОЗТ «Инвестинформ» /115583, Москва, ул. Ясеневая, 19-3-265,т. 299-9830 /3в, г, д, е /Срок действия истек

133 /ЛГ0013, 000633 /№ 133 /26.10.95 /26.10.2001 /Государственное предприятие - Научно-производственное объединение «Импульс» (НПО «Импульс») (РКА) /195220, Санкт-Петербург, ул. Обручевых, 1, т. (812) 247-5701, 552-9521 /1.2а-ж;2;3;4; 5а-в /Продлено

134 /ЛГ 0004, 000165 /№ 134 /26.10.95 /16.9.2001 /ООО «Частное охранное предприятие «ФОРТ» (ЧОП «ФОРТ») /103903, Москва, Большой Кисловский пер., 1-1-12,стр.2, т.280-4522 /2;3.3-Э.9»-в;4 /Продлено и изменено

135 /ЛГ0013, 000635 /№ 135 /26.10.95 /26.10.2001 /Научно-исследовательский институт измерительных систем (ЦНИИИС) (Минатом России) /603600, Нижний Новгород, ГСП-486, НИИИС, т. (831-2) 66-16-20, 66-49-90 /1.2а-в;2а-е; 3.4-3.9а-в; 4 /Продлено

136 /ЛГ0013, 000648 /№ 136 /02.02.96 /02.02.99 /ООО «Спецтехника» /198052, Санкт-Петербург, а/я 8, ул. Мичуринская, 1, т. 233-0648 /3.3а-в; 3.9а-в /

137 /ЛГ0013, 000637 /№ 137 /02.02.96 /02.02.99 /АООТ «Информационные телекоммуникационные технологии» (ИНТЕЛТЕХ) /197342, Санкт-Петербург, ул. Кантемировская, 6, т. 245-5069 /2; 3; 4; 5а-в /

138 /ЛГ0013, 000638 /№ 138 /02.02.96 /02.02.99 /АООТ «Институт по проектированию предприятий машиностроения и приборостроения» (ПРОЕКТМАШПРИБОР)/129085, Москва, Звездный б-р, 19,т.217-4093,217-2966 /5 /

Продолжение приложения 3

№ п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки

139 /ЛГ0013, 000639 /№ 139 /02.02.96 /14.04.98 /АООТ «Межгосударственная акционерная корпорация «Вымпел» /101000, Москва, а/я 83, 4-я улица 8-го Марта, 3, т. 152-4496 /2; 3.4-3.9а-в; 4 /Срок действия истек

140 /ЛГ0013, 000640 /№ 140 /02.02.96 /02.02.99 /Научно-производственное предприятие «Кант» (НПО «Кант») (Минэкономики России) /109004, Москва, Товарищеский пер., 31, стр.1, т. 912-5515 /3.4-3.9а-б /

141 /ЛГ0013, 000641 /№ 141 /02.02.96 /02.02.99 /ТОО «Научно-производственное предприятие «КОМТЭР» (НПО «КОМТЭР») (Минэкономики России) /109004, Москва, Товарищеский пер., 31, стр.1, т. 912-2499 /3.4-3.9а-б /

142 /ЛГ0019, 000942 /№ 142 /06.02.96 /06.02.99 /ЗАО «АЭРОСОФТ» /117330, Москва, ул. Мосфильмовская, 176, т.330-8077 /3а, б, г, д /

143 /ЛГ0013, 000643 /№ 143 /13.02.96 /13.02.99 /Общественная организация «Ассоциация разработчиков информационных и управляющих

систем» /196070, Санкт-Петербург, ул. Победы, 4, т. (812) 108-3863 /3;4 /

144 /ЛГ0013, 000644 /№ 144 /13.02.96 /20.02.2001 /Казанский научно-исследовательский институт радиоэлектроники (НИИ РЭ) (Минэкономики России) /420029, Казань, ул. Журналистов, 50/3, т. (8432) 76-76-93, 76-45-94 /26, г, д, е; 3а, б, г, с; 4 /Продлено

145 /ЛГ0013, 000645 /№145 /20.02.96 /20.02.99 /Санкт-Петербургский государственный электротехнический университет им. Ленина (Минобразования России) /197376, Санкт-Петербург, ул. Профессора Попова, 5, т. (812) 234-6293, 234-8947 /1.2а-в;2;3;4;б /

146 /ЛГ0013, 000646 /№ 146 /06.03.96 /06.03.99 /АОЗТ «Научно-исследовательский институт «ЦЕНТРПРОГРАММСИСТЕМ» /170650, ГСП, Тверь, пр. 50 лет Октября, 3, т. 44-95-30,44-32-44 /3а-г,е /

147 /ЛГ0013, 000647 /№ 147 /20.02.96 /20.02.99 /АОЗТ «МХМ-ЕНИСЕЙ» /660028, Красноярск, ул. Мечникова, 49, , т. 43-63-88,43-57-60 /3.3-3.9а-е /

148 /ЛГ0001, 000005 /№ 148 /04.11.97 /04.11.2000 /ООО«САЙКОМ» /119501, Москва, ул. Матвеевская, 6, т. 124-4194,332-1115 /3.3а, в, г /

149 /ЛГ0013, 000649 /№ 149 /13.02.96 /13.02.99 /АООТ «ГИПРОНИИАВИАПРОМ» (Минэкономики России) /125083, Москва, ул. Верхняя Масловка, 20, т. 212-5121,212-9358 /2.1; 5 /

150 /ЛГ0013, 000650 /№ 150 /13.02.96 /13.02.99 /АОЗТ «РОССОШЬ» /142092, Московская обл., Троицк, Центр научно-технической деятельности РАН «ОМИКРОН», а/я 1 Б, пом.7, т. 240-2002/3.3-3.4г-д; 3.6-3.7г-д; 3.9г-д /

Продолжение приложения 3

№ п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки

151 /ЛГ0014, 000651 /№151 /04.03.96 /04.03.99 /АОЗТ «Всесоюзный институт волоконно-оптических систем связи и обработки информации» /107066, Москва, ул. Нижняя Красносельская, 13,корп.1, т. 267-2031,267-3383 /1.2; 2,3,4; 5»-» /

152 /ЛГ0014, 000652 /№ 152 /04.03.96 /04.03.99 /АОЗТ «Научно-производственное предприятие «Пульсар» (НПП ПУЛЬСАР) /117981, Москва, пр. Вернадского, 41, т. 430-8325 /2; 3а,в-е; 5а-в /

153 /ЛГ0014, 000653 /№ 153 /04.03.96 /04.03.99 /ОАО «Московская городская телефонная сеть» (МГТС) /103804, Москва, ГСП, Дегтярный пер., 6,стр.2, т. 299-2885 /2; 3.3-3.4г-ж; 3.7г-ж; 3.9г-ж; 4; /

154 /ЛГ0014, 000654 /№ 154 /04.03.96 /04.03.99 /ТОО «МЕХЭЛЕКТРОН» /113191, Москва, Холодильный пер., 1, т. 955-2763, 955-2509 /1.2г-е; 2а-г;3г-е /

155 /ЛГ0014, 000655 /№ 155 /04.03.96 /04.03.99 /АОЗТ «Атлас-Контакт» /197198, Санкт-Петербург, ул. Гатчийская, 16, Т.(812)230-9704 /3.1-3.5г-е;3.9г-е /

156 /ЛГ0014, 000656 /№ 156 /06.03.96 /06.03.99 /ТОО «Научно-техническое предприятие «КРИПТОСОФТ» /440601, Пенза, ул. Советская, 9, т. 69-07-41 /1.2;2а-в;3;4 /

157 /ЛГ0014, 000657 /№ 157 /06.03.96 /06.03.99 /ТОО «Научно-производственное предприятие «АЛЬТАНТ» /111024, Москва, ул. Авиамоторная, 57, т. 273-6576 /2; 4 /

158 /ЛГ0014, 000658 /№ 158 /06-03.96 /06.03.99 /АООТ «Ижевский радиозавод» (Минэкономики России) /Удмуртская Республика, 426034, Ижевск, ул.6азисная,19, т. 22-70-10 /2; 3а-в;4 /

159 /ЛГ0014, 000659 /№ 159 /06.03.96 /06.03.99 /ООО «Сатурн-Каскад»

/107553, Москва, ул. Большая Черкизовская, 103/105, т. 161-2000 /3.5-3.6а-б /

160 /ЛГ0014, 000660 /№ 160 /06.03.96 /06.03.99 /АООТ «МТУ Сатурн» /107553, Москва, ул. Большая Черкизовская, 103/105, т. 161-2000 /3.5-3.6а, б, г; 3.9а, б, г /

161 /ЛГ0014, 000662 /№ 161 /21.03.96 /21.03.99 /Научно-производственное предприятие «КИРСИ» научно-производственного объединения «Радиевый институт им. В. Г. Хлопина» (Минатом России) /194021, Санкт-Петербург, 2-й Мичуринский пр., 28, т. 232-7039 /1.2а-в;2;3а,в /

162 /ЛГ 0014, 000663 /№ 162 /21.03.96 /21.03.99 /Концерн «Системпром» /107066, Москва, ул. Нижняя Красносельская, 13, корп. 1, т. 267-2031 /1.2м; 2,3; 4; 5а-в /

163 /ЛГ 0014, 00062/№ 163 /21.03.96 /21.03.99 /АООТ «Научно-исследовательский институт систем автоматизации» (НИИ СА) /109316, Москва, Волгоградский пр., 2, т. 274-9443, 274-9000 /1.2б,г-е;2а-б,р-д; 1.1а-б,г; 3.3-3.9а,б,г-е; 4; 5а-в /

Продолжение приложения 3

№ п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки

164 /ЛГ0014, 000665 /№ 164 /21.03.96 /21.03.99 /ОАО «ИнфоТеКС» /125047, Москва, а/я 190, т. 158-2893,943-9210 /3.1-3.4г-е; 3.6-3.7г-е; 3.9г-е /

165 /ЛГ0014, 000666 /№ 165 /26.03.96 /26.03.99 /ООО «АНКЕЙ» /119833, Москва, ул. Погодинская, 10, стр.1, т.247-1999 /2.2; 3.1-3.4; 3.7; 3.5а-в; 3.6а-в; 3.8-3.9а-в; 4; 5 /

166 /ЛГ0014, 000667 /№ 166 /27.03.96 /27.03.99 /Государственное научно-производственное объединение «Альтаир» (Минэкономики России) /111024, Москва, ул. Авиамоторная, 57, т. 273-1432 /2; 4 /

167 /ЛГ0014, 000668 /№ 167 /27.03.96 /27.03.99 /Научно-технический центр «Заря» (НТЦ «Заря») (Минэкономики России) /125889, Москва, ГСП-47, Миусская площадь, 3, т. 251-3767,252-9682 /2; 3.3-3.9а-д; 4; 56 /

168 /ЛГ0014, 000669 /№ 168 /27.03.96 /27.03.99 /АООТ «СеверЭВМкомплекс» /195272, Санкт-Петербург, пр. Шаумяна, 18? Т.(812)164-1465, 164-1797 /1.2; 2; 3:4 /

169 /ЛГ0014, 000670 /№ 169 /28.03.96 /28.03.99 /Управление президентской связи Главного управления охраны РФ /103012, Москва, ул. Никольская, 6/2, т. 224-0579, 224-3711 /2;3.1-3.4а-в; 3.7а-в; 3.9а-в; 4; 56, д, е /

170 /ЛГ0014, 000671 /№170 /11.04.96 /11.04.2001 /Научно-исследовательский институт автоматики (НИИА) (Минэкономики России) /127106, Москва, ул.Ботаническая, 25, т. 219-3543, 219-2904 /1.2а-е;2;3а-е;4; 5а-в /

171 /ЛГ0014, 000672 /№ 171 /11.04.96 /11.04.99 /ТОО «КОРТА» /344022. Ростов-на-Дону, ул. Максима Горького, 245, т. 53-79-44 /3.2-3.66, д; 3.8-3.96,д /

172 /ЛГ0014, 000673 /№ 172 /11.04.96 /11.04.99 /ТОО «Научно-производственный центр «СИБ» /189510, Санкт-Петербург, Ломоносов, ул. Жоры Антоненко, 16, кв.2, Т.(812)427-9777 /3 /

173 /ЛГ0014, 000674 /№ 173 /16.04.96 /16.04.99 /АОЗТ «Научно-технический центр «РАСТР» /630132, Новосибирск, ул. 1905 года, 13,т.21-8484,21-1859 /2.1д-е;3.1-3.3а; 3.5а; 3.7-3.9а /

174 /ЛГ0014, 000675 /№ 174 /16.04.96 /16.04.99 /Войсковая часть 77111 (Минобороны России) /103160. Москва, К-160, в/ч 77111, т. 296-3001,296-3000 /1.2а-в; 2; 3.7а-в; 3.9а-в;4 /

175 /ЛГ0014, 000676 /№ 175 /16.04.96 /16.04.99 /Войсковая часть 55387 (Минобороны России) /103160, Москва, К-160, в/ч 55387, т. 293-6633,293-6638 /1.2а-в; 2; 3.7а-в; 3.9а-в;4 /

176 /ЛГ0014, 000677 /№ 176 /16.04.96 /16.04.99 /000 «Агентство «Навигатор» /103527, Москва, Зеленоград, корп. 814,7 эт., т. 530-0869 /3.3-3.4г;3.9г /

Продолжение приложения 3

№ п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки

177 /ЛГ0014, 000678 /№ 177 /16.04.96 /16.04.99 /Центральный НИИ машиностроения (РКА) /141070, Калининград Московской обл., ул. Пионерская, 4, т. 513-5635 /2а-в, д; 3.1 а-б, г-е; 3.3-3.4а, б, г-е; 4 /

178 /ЛГ0014, 000679 /№ 178 /16.04.96 /16.04.99 /Государственное предприятие Научно-исследовательский институт «Масштаб» (НИИ «Масштаб») (Минэкономики России) /197342, Санкт-Петербург, ул. Кантемировская, 5, т. 245-0311,245-5165 /26, в, д, е; 3.1-3.2а,б,г-е; 3.4-3.7а, б, г-е; 3.9а-б, г-е; 4 /

179 /ЛГ0014, 000680 /№ 179 /18.04.96 /18.04.99 /ЗАО «Научно-производственное объединение «РЕМСТРОЙЭКОЛОГИЯ» /Москва, Ореховый проезд, 9, кв.59, т.452-0400 /2; 4 /

180 /ЛГ0014, 000681 /№ 180 /18.04.96 /18.04.99 /000 «Предприятие «ОРА-ЦЕНТР» /107061, Москва, ул. Б.Черкизовская, 16/2, стр.1, пом.2 (кв.4), т.963-7789,963-8332 /3.1г-е;3.3-3.4г-е; 3.б-3.7г-е; 3.9г-е; 5а-в /

181 /ЛГ 0007, 000338 /№ 181 /26.03.97 /26.03.99 /Конструкторское бюро «Селена» (Минэкономики России) /350072, Краснодар, ул. Московская, 81, т. 54-55-52, 54-02-27 /2а, б, г, д, е; 3.1-3.8а,б; 3.9а, б, г; 4 /

182 /ЛГ0014, 000684 /№ 182 /24.04.96 /24.04.99 /Главный научно-информационный вычислительный центр Государственного таможенного комитета РФ (ГНИВЦ ГТК) /107842, Москва, Комсомольская пл., 1-А, т. 975-4745 /2; 3; 4; 5а-в /

183 /ЛГ0014, 000685 /№ 183 /24.04.96 /24.04.99 /ЗАО «Научно-производственное объединение спецтехники «Классик» /109052, Москва, ул. Подъемная, 12,т.918-0380 /3а, г, д, е /

184 /ЛГ0014, 000686 /№ 184 /29.04.96 /29.04.99 /Научно-исследовательский институт системных исследований Российской Академии наук (НИИСИ РАН) /109280, Москва, ул. Автозаводская, 23, т.277-2710,274-6333 /2а-г; 3а-в, ж; 4 /

185 /ЛГ0014, 000687 /№ 185 /07.05.96 /07.05.99 /АОЗТ «Научно-промышленное общество «НАУТЕКС» /109316, Москва, Волгоградский пр., 2, т. 274-9316 /1.26, г-е; 2а, б, г, д; 3.1а,б,г-е; 3.3-3.9а, б, г-е; 4; 5а-в /

186 /ЛГ0014, 000688 /№186 /07.05.96 /07.05.99 /ТОО «Программно-технический центр «ДЕЛОНА» /630118,Новосибирск, ул. Б.Богаткова, 228/1, корп. 207, т.63-1490 /2;3г,д,е;4 /

187 /ЛГ0014, 000689 /№ 187 /07.05.96 /07.05.99 /АОЗТ «Научно-производственное предприятие «РЕГИОН-РК» /630132, Новосибирск, ул. 1905 года, 13, т. 21-0730 /2.2а-е /

Продолжение приложения 3

№ п/п /Серия, номер бланки /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки

188 /ЛГ0014, 000690 /№ 188 /15.05.96 /15.05.99 /АОЗТ «ИРКОС» /129626,

Москва, а/я 30, АОЗТ «ИРКОС», т.287-7892,217-2911 /3; 5а-в /

189 /ЛГ0014, 000692 /№ 190 /16.05.96 /16.05.99 /АООТ «Центральный телеграф» /103375, Москва, ул. Тверская, 7, т. 201-9178, 924-9004 /2; 3.1; 3.3-3.9;4 /

190 /ЛГ0014, 000693 /№ 191 /16.05.96 /16.05.99 /ТОО Компания «ТЕКОС Лтд.» /141070, Калининград Московской обл., ул. Пионерская, 4, т.251-1293 /3.1г-е;3.3г-с /

191 /ЛГ0014, 000694, /№ 192 /23.05.96 /23.05.99 /Российский федеральный ядерный центр — Всероссийский научно-исследовательский институт экспериментальной физики (РФЯЦ — ВНИИЭФ) (Минатом России) /607190, Саров (Арзамас-16), Нижегородской обл., пр. Мира, 37,т. 83130-51800 S. /1.2а-в;2;3;4; 5а-в /

192 /ЛГ0014, 000695 /№ 193 /23.05.96 /23.05.99 /ООО «Фирма «ЛИМЕС» /113405, Москва, Варшавское ш., 125, офис 617, т. 755-5950 /3.1-3.4г-д; 3.9г-д /

193 /ЛГ0014, 000696 /№ 194 /23.05.96 /23.05.99 /Специализированное конструкторское бюро «ВОСТОК» (СКБ «ВОСТОК») (Минэкономики России) /656002, Барнаул, пр. Калинина, 15, т. 77-09-97,77-00-89 /2; 4 /

194 /ЛГ0014, 000697 /№ 195 /30.05.96 /30.05.99 /ЗАО «СЕТ-1» /103473, Москва, 1-й Самотечный пер., 17А, РЦТМ, т. 288-6706 /2:3; 4; 5 /

195 /ЛГ0014, 000698 /№ 196 /30.05.96 /30.05.99 /ООО «Центр информационной безопасности «Альтернатива» /443068, Самара, пос. Кр. Глинка, квартал 4, 10, кв.40,т.22-14-76 /2; 3а-е; 4; 5 /

196 /ЛГ0014, 000699 /№ 197 /30.05.96 /30.05.99 /Центр технических систем передачи информации при МИД России /121200, Москва, Смоленская-Сенная пл., 32/34, т. 244-2214 /2; 3.4-3.6а-в; 3.8-3.9а-в;4 /

197 /ЛГ0014, 000700 /№ 198 /30.05.96 /30.05.99 /Акционерная компания «Международное сотрудничество и сервис металлургов «ИНТЕРМЕТСЕРВИС» /103718, Москва, Славянская пл.,2, т. 220-7251,220-7067 /2;3.4-3.9а-в; 4 /

198 /ЛГ 0009, 000401 /№ 199 /03.06.96 /03.06.99 /ООО «Научно-производственное предприятие «СИТЕКС» /107066, Москва, ул. Старая Басманная, 21, т. 263-9877 /2; 3; 4; 5а-в /

199 /ЛГ 0009, 000402 /№200 /16.07.96 /16.07.99 /АОЗТ «Инфосистемы Джет» /103006, Москва, Краснопролетарская, 6, т. 972.1182, 973-4848 /3.3-3.7г-ж; 3.9г-ж;5а-б /

Продолжение приложения 3

№ п/п /Серия, номер бланка /Номер лицеи- /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки

200 /ЛГ 0009, 000403 /№201 /04.06.96 /04.06.99 /АООТ «ВЕЛТА» /614025, Пермь, ул. Героев Хасана, 105,т.49-42-89 /2; 3.2а; 3.3а-в; 3.5а-б; 3.7а-б; 3.9а-б; 4 /

201 /ЛГ0009, 000404 /№202 /04.06.96 /04.06.99 /Центральное конструкторское бюро «Титан» (ЦКБ «Титан») (Минэкономики России) /400071, Волгоград-71, пр. им. В. И. Ленина, т. 71-19-10 /2.1а,в-е;2.2г-е; 3.1г;3.4а-в,г; 3.5а; 3.9а /

202 /ЛГ0009, 000405 /№203 /06.06.96 /06.06.99 /Государственное предприятие Научно-исследовательский институт «Рубин» (Минэкономики России) /197342, Санкт-Петербург, ул. Кантемировская, 4, т. (812) 245-0129 /2;3а-б,г-ж;4 /

203 /ЛГ0009, 000406 /№204 /06.06.96 /06.06.99 /АООТ «Московский вертолетный завод им. М. Л. Миля» (Минэкономики России) /107113, Москва, Сокольнический вал, 2, т. 264-5403 /2а-б, г-е; 3.4-3.9а-в; 4 /

204 /ЛГ 0009, 000407 /№205 /06.06.96 /06.06.99 /000 «Сюртель» /107078, Москва,. Большой Харитоньевский пер., 21/6, стр. 2, пом. правления, т. 261-6179 /2; 3а-в /

205 /ЛГ0009, 000408 /№206 /11.06.96 /11.06.99 /000 «ЛАН Крипто, Лтд.» /117321, Москва, ул. Профсоюзная, 130, корп.2, комн. правления, т. 288-5056, 288-5388 /3.1-3.4г-е;3.6г-е; 3.9г-е /

206 /ЛГ 0009, 000409 /№207 /11.06.96 /11.06.99 /АООТ «ВНИПИнефть» /113813, Москва, ул. Димитрова, 33/13, т. 238-1221 /2д; 3.3-3.4а; 4 /

207 /ЛГ 0009, 000410 /№208 /24.06.96 /24.06.99 /АООТ «Научно-исследовательский институт вычислительных средств «Спектр» (НИИВС «Спектр») /196066, Санкт-Петербург, Московский пр., 212, т.291-3329, 264-1239 /3а,в-е /

208 /ЛГ 0009, 000411 /№209 /01.07.96 /01.07.99 /ИЧП «АЛЬБА» /123458, Москва, ул. Таллинская, 2, кв. 24,т.942-4204 /2.1а, б;3г-ж /

209 /ЛГ 0009, 000412 /№210 /01.07.96 /01.07.99 /Волгоградский государственный технический университет (Минобразования России) /400066, Волгоград, пр. В. И. Ленина, 28, т. 34-00-76 /6 /

210 /ЛГ 0009, 000413 /№211 /08.07.96 1 /08.07.99 /ЗАО «Московское отделение Пензенского научно-исследовательского электротехнического института» (МО ПНИЭИ) (ФАПСИ) /127018, Москва, ул. Образцова, 38, т. 289-4361,289-3493 /1.2а-ж;2а-е; 3а-ж; 4; 5а-в /

211 /ЛГ 0009, 000414 /№212 /15.07.96 /15.07.99 /Малое государственное научно-производственное предприятие «Ферро-Центр» /196084, Санкт-Петербург, ул. Черниговская, 8, т. (812) 294-7125; 298-7915 /3а-в; 4 /

Продолжение приложения 3

№ п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особыеотметки

212 /ЛГ 0009, 000415 /№213 /16.07.96 /16.07.99 /ТОО «ФОРТЕ» /344007, Ростов-на-Дону, ул.6аумана,64, т. 63-52-36,62-38-79 /3.3-3.9а,б,г,д /

213 /ЛГ0009, 000416 /№214 /24.07.96 /24.07.99 /ТОО «ПРОГРЕССТЕХ Лтд.» /109210, Москва, Покровский б-р, 3, т. 206-6336 /2;3;4 /

214 /ЛГ 0009, 000417 /№215 /24.07.96 /24.07.99 /ЗАО «ГРАНТ-СИСТЕМЫ И ТЕХНОЛОГИИ» /105215. Москва, ул. 9-я Парковая, 53, т. 164-4769 /2; 3; 4; 5а-в /

215 /ЛГ 0009, 000418 /№216 /24.07.96 /24.07.99 /ТОО «ИНЦИАЛ» /129110, Москва, пр. Мира, 57, т. 155-3641 /2; 3а-е;4 /

216 /ЛГ 0009, 000419 /№217 /24.07.96 /24.07.99 /ОАО «Ижевский мотозавод «АКСИОН» /426006, Ижевск, Удмуртская республика, ул. Максима Горького, 90, т. 250-466 /2б-е; 3а, в-е; 4; 5д-е /

217 /ЛГ 0009, 000420 /№218 /26.07.96 /26.07.99 /Государственная компания по экспорту и импорту вооружений и военной техники «РОСВООРУЖЕНИЕ» /119865, Москва, Гоголевский б-р, 21, т. 202-3673 /2г-е; 3.3- 3.6а-в; 3.9а-в /

218 /ЛГ 0009, 000421 /№219 /31.07.96 /31.07.99 /Филиал Пензенского научно-исследовательского электротехнического института НИП «АРГУС» /440601, Пенза, ул. Советская, 9, т. 55-3700, 89-0783 /3; 5а-в /

219 /ЛГ 0009, 000422 /№220 /31.07.96 /31.07.99 /ТОО «Научно-производственное предприятие «РОКАДА» /440601, Пенза, ул. Советская, 9, т. 69-0765, 66-4291 /3; 5а-в /

220 /ЛГ 0009, 000423 /№221 /31.07.96 /31.07.99 /ОАО «Специализированное монтажно-наладочное управление № 70» ПМСП «Электрон» (Минатом России) /630065, Новосибирск-65, СМНУ №70, т. 74-4572, 76-1331 /3.3-3.6а, б, г; 3.9а, б, г; 5а, б, д /

221 /ЛГ 0009, 000424 /№222 /01.08.96 /01.08.99 /Войсковая часть 49456 (Минобороны России) /125284, Москва, А-284, в/ч 49456, т. 941-3844,941-3731 /1.2;2а-д;3;4; 5а-в /

222 /ЛГ 0009, 000425 /№223 /01.08.96 /01.08.99 /Российский государственный гуманитарный университет (Минобразования России) /Москва, ул. Кировоградская,25, корп. 2, т. 388-0881, 387-2018 /2;3.1г-ж; 3.3-3.4г-ж; 3.9г-ж; 4; 6 /

223 /ЛГ 0009, 000426 /№224 /01.08.96 /01.08.99 /ГУП «Специальное агентство экспертизы, лицензирования, сертификации и аттестации «ОМЕГА» (Минэкономики России) /195220, Санкт-Петербург, ул. Обручевых, 1, т. (812) 247-5701, 247-5865 /1.2а-г;2;3;4; 5а-в /

224 /ЛГ 0009, 000427 /№225 /01.08.96 /01.08.99 /000 «Научно-производственное и инновационное объединение «ТОНАРМ» /195220, Санкт-Петербург, ул. Обручевых, 1, т. 552-9740, 552-9840 /2; 3; 4; 5а-в /

Продолжение приложения 3

№ п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки

225 /ЛГ 0010, 000497 /№226 Дубликат /05.08.96 /05.08.99 /ТОО «Триада Про» /125008, Москва, а/я 215 ул. Михалковская, 7, т.153-5033,153-1624 /2; 3,4; 5а-в /

226 /ЛГ 0009, 000429 /№227 /15.08.96 /15.08.99 /АООТ «ЭЛВИС+» /103460, Москва, Зеленоград, Центральный пр., 11, т.531-4633 /2.2; 3г-е; 5а-в /

227 /ЛГ 0009, 000430 /№228 /15.08.96 /15.08.99 /Государственное научно-производственное предприятие «Полет» (Минэкономики России) /603600, Нижний Новгород, Комсомольская пл., 1, т. 42-35-29, 42-21-04 /2. 1а, б, г, д; 3а, б, г, е; 4; 5а-б /

228 /ЛГ 0009, 000431 /№229 /15.08.96 /15.08.99 /Научно-исследовательский институт систем связи и управления (НИИ ССУ) (Минэкономики России) /117630, Москва, Старокалужское ш., 58, т.333-7503,330-8622 /2; 3.1-3.9; 4; 5а-в /

229 /ЛГ0009, 000432 /№230 /19.08.96 /19.08.99 /ТОО «ИНИСТ» /117419, Москва, ул. Орджоникидзе, 11, т.955-1616,955-1521 /3г-е /

230 /ЛГ 0009, 000433 /№231 /19.08.96 /19.08.99 /Войсковая часть 35533 /143980, Железнодорожный-8, Московская обл., в/ч 35533, т. 522-5652 /2;3;4;5 /

231 /ЛГ 0009, 000434 /№232 /06.09.96 /06.09.99 /000 «Центурион Системе» /119619, Москва, Боровский проезд, 6, кв.36 /2; 3; 4; 5а-в /

232 /ЛГ 0009, 000435 /№233 /11.09.96 /11.09.99 /ТОО «Фирма «Радиокоммуникации и компьютеры» (Фирма РКК) /109072, Москва, Болотная набережная, 15, т. 230-3132, 230-3136 /3а, б, в, ж /

233 /ЛГ 0009, 000436 /№234 /11.09.96 /11.09.99 /ЗАО «Научно-производственное объединение космического приборостроения» (РКА) /111250, Москва, ул. Авиамоторная, 53, т.273-9613,273-9889 /2а, д; 3.4а, б; 4 /

234 /ЛГ 0009, 000437 /№235 /11.09.96 /11.09.99 /ГП «Марийский машиностроительный завод» (Минэкономики России) /424003, Йошкар-Ола, ул. Суворова, 15, т.9-3137,9-3466 /2;3.3-3.7а-в;4 /

235 /ЛГ 0009, 000438 /№236 /11.09.96 /11.09.99 /ТОО«АМИКОН» /101000, Москва, Чистопрудный б-р, 12-А, т. 220-8847 /3г-е /

236 /ЛГ 0009, 000439 /№237 /12.09.96 /12.09.99 /000 «Аттестационный центр «ВЕТЕРАН» /125167, Москва, Ленинградский пр., 40, академия им. Жуковского, т. 155-1698 /2; 3.3-3.66, г; 3.96, г; 4 /

237 /ЛГ0009, 000440 /№238 /19.09.96 /19.09.99 /ГП «Красноярский

машиностроительный завод» (Минэкономики России) /660123, Красноярск, пр. им.газеты «Красноярский рабочий», 29,т.33-4891,33-2829 /2; 3.3-3.7; 3.8-3.9а-в; 4 /

Продолжение приложения 3

№ п/п /Сери», номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки

238 /ЛГ 0009, 000441 /№ 239 /19.09.96 /19.09.99 /Служба безопасности Российского акционерного общества «Газпром» /117884, ГСП, Москва, В-420, ул. Наметкина, 16, т.719-2741,719-2084 /26, г, д, е; 3.4-3.6а-б; 4 /

239 /ЛГ0009, 000442 /№240 /19.09.96 /19.09.99 /ЗАО «Релком-Альфа» /123060, Москва, ул. Расплетина, 4, корп. 1, т. 198-3796, 196-7221 /3а-ж /

240 /ЛГ0009, 000443 /№241 /19.09.96 /19.09.99 /АООТ «Центральный научно-исследовательский институт радиоэлектронных систем» (ЦНИИРЭС) (Минэкономики России) /129110, Москва, пр. Мира, 69, т.281-4797,288-5880 /2;3;4 /

241 /ЛГ 0009, 000444 /№242 /25.09.96 /25.09.99 /ЗАО «Частное охранное предприятие» /101000, Москва, ул. Мясницкая, 14, т. 923-9473,923-8612 /2; 3.3-3.9;4;5 /

241 /ЛГ 0009, 000445 /№243 /30.09.96 /30.09.99 /ООО «ФОРТУНА-ИНВЕСТ» /113639, Москва, Варшавское ш.,402, кв. 9, т. 267-7095 /2д, е; 3а; 5а-в /

243 /ЛГ0009, 000446 /№244 /30.09.96 /30.09.99 /ТОО «КОМИНФОР» /127577, Москва, ул. Бестужевых, 13,кв.207,т.258-4170 /3 /

244 /ЛГ 0009, 000447 /№245 /07.10.96 /07.10.99 /ЗАО «РОКСА» /123056, Москва, ул. Красина, 17, а/я 63,т.178-9626,200-8619 /3.56; 3.96; 5а-д /

245 /ЛГ 0009, 000448 /№246 /07.10.96 /07.10.99 /Информационно-вычислительный комплекс Российского научного центра «Курчатовский институт» /123182, Москва, пл. Академика Курчатова, 1,эд.101,т. 196-9373 /2; 3;5а-в /

246 /ЛГ0009, 000449 /№247 /07.10.96 /07.10.99 /Пензенский научно-исследовательский электротехнический институт (ПНИИЭИ) (ФАПСИ) /440601, Пенза, ул. Советская, 9, т. 69-07-40, 66-16-86 /1.2; 2; 3; 4; 5а-в /

247 /ЛГ 0003, 000110 /№248 /07.10.96 /07.10.99 /ООО «КОМИС» /424015, Йошкар-Ола, ул. Первомайская, 166,14-й этаж, т. (8362) 12-08-10,12-67-41 /2.1г-е;3.1-3.2а-в; 3.3-3.4а-е; 3.5а, б, г; 3.6а-е; 3.9а-е; 4; 5а-в /Замена бланка (переименование)

248 /ЛГ0010, 000451 /№249 /07.10.96 /07.10.99 /АОЗТ «ГЕНКЕЙ» /107014, Москва, ул. Большая Оленья, 15а, т. 168-9824 /2; 3а-е; 4; 5а-в /

249 /ЛГ0010, 000452 /№250 /15.10.96 /15.10.99 /Воронежский государственный технический университет (Минобразования России) /394026, Воронеж, Московский пр., 14, т. 13-08-96, 16-29-90 /б /

250 /ЛГ0010, 000453 /№251 /18.10.96 /18.10.99 /ЗАО «Особое конструкторское бюро «Сатурн» (ОКБ «Сатурн») /107553, Москва, ул. Большая Черкизовская, 103/105, т. 161-8211/2а,б,г,д,е;3.1б; 3.4-3.66; 4 /

Продолжение приложения 3

№ п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки

251 /ЛГ0010, 000454 /№252 /22.10.96 /22.10.99 /ООО «КОМПАНИЯ СТЭН» /117330, Москва, ул. Мосфильмовская, 35, стр.1, т. 232-3610 /3.3-3.96,

г, д; 5а-в /
252 /ЛГ0010, 000455 /№253 /22.10.96 /22.10.99 /Государственное производственное объединение «Завод им. М. И. Калинина» (Минэкономики России) /199155, Санкт-Петербург, ул. Уральская, 1, т. 350-8936, 350-1354 /2.26-е; 3.26; 4 /
253 /ЛГ0010, 000456 /№254 /31.10.96 /31.10.99 /ЗАО «Компания «Оверком Сеть» /125040, Москва, ул. Скаковая, 32, стр.2,т.945-5458 /3.1-3.4г,д; 3.9г, д /
254 /ЛГ0010, 000457 /№255 /31.10.96 /31.10.99 /ЗАО «Межотраслевой научно-технический центр «ТЕЗИС» /109462, Москва, Волжский б-р, кв-а 113а, корп.7, комн. правления, ЖСК «Тульский», т.190-7765/2; 3а-в;4 /
255 /ЛГ0010, 000458 /№256 /31.10.96 /31.10.99 /Российский научно-исследовательский институт космического приборостроения (РНИИ КП) (РКА) /111250, Москва, ул. Авиамоторная, 53, т. 273-9611,273-9601 /2а,д; 3.4а,б;4 /
256 /ЛГ0010, 000459 /№257 /31.10.96 /31.10.99 /ЗАО «АСС.СПЕЙС ТВ» (РКА) /105215, Москва, ул. 13, Парковая, 27, корп.4, комн. правления, т.273-9630,273-9889 /2а, д; 3.4а, б; 4 /
257 /ЛГ0010, 000460 /№258 /04.11.96 /04.11.99 /ТОО «БИЗОН Лтд.» /607190, Саров Нижегородской обл., а/я 54 /2;3;4 /
258 /ЛГ0010, 000461 /№259 /05.11.96 /05.11.99 /ГП «Главный научно-исследовательский вычислительный центр Минприроды России (ГлавНИВЦ) (Минприроды России) /123585, Москва, ул. Тухачевского, 32, корп. А, т. 192-8017, 192-8015 /2; 3.3-3.4а-е; 3.5-3.6а-в; 3.7а-е; 3.8а-в; 3.9а-е; 4; 5а-в /
259 /ЛГ0010, 000462 /№260 /04.11.96 /04.11.99 /ЗАО «Научно-производственный центр «РИФ-ЗАЩИТА» /630075, Новосибирск, ул. Объединения,3, т. 74-12-55,74-25-93 /1;2;3;4;5а /
260 /ЛГ0010, 000463 /№261 /05.11.96 /05.11.99 /000 «СИДДХИ-СЕКЪЮРИТИ» /420012, Казань, а/я 92 ул. Журналистов, 1/16, корп. 201, т. 75-35-03 /2; 3,4 /
261 /ЛГ0010, 000464 /№262 /21.11.96 /21.11.99 /ЗАО «Научно-внедренческое предприятие «ПРОТЕК» /394051, Воронеж, ул. Домостроителей, 30, т. 72-27-64,72-27-65 /3а, б /
262 /ЛГ0001, 000025 /№263 /21.11.96 /21.11.99 /ЗАО «РИКА ИНЖИНИРИНГ» /101000, Москва, Колпачный пер., 6, стр.7, т. 925-9028, 160-9753 /2; 3.3-3.9; 4; 5а-в /
Продолжение приложения 3
№ п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки
263 /ЛГ0010, 000466 /№264 /21.11.96 /21.11.99 /Инновационный коммерческий банк «АЛЬФА-БАНК» /107078, Москва, ул. Маши Порываевой, 11, т. 204-9009 /2; 3.3-3.9а, б; 4 /
264 /ЛГ0010, 000467 /№265 /27.11.96 /27.11.99 /ГП «Казанское объединение по производству средств вычислительной техники «Терминал» /420029, Казань, ул. Сибирский тракт, 34, т. 76-22-23, 76-21-73 /36, г, д, е, ж; 3.3-3.5а,в; 3.6а /
265 /ЛГ0010, 000468 /№266 /27.11.96 /27.11.99 /ТОО «Апрель» /400066, Волгоград, ул. Волгодонская, 7, т, 33-96-21 /3.3-3.96 /
266 /ЛГ0007, 000325 /№267 /04.12.96 /04.12.99 /000 «Фирма «АНКАД» /103482, Москва, НИИТТ, фирма «АНКАД», т. 532-9649, 534-5669 /3.1-3.4г-е; 3.6-3.9г-е /
267 /ЛГ0010, 000470 /№ 268 /04.12.96 /04.12.99 /АОЗТ «Диалог-Наука»

/117967, Москва, ул. Вавилова, 40, ВЦ РАН, т. 938-2970 /3г, д, е, ж /
268 /ЛГ0010, 000471 /№269 /06.12.96 /06.12.99 /Новосибирский государственный технический университет (Минобразования России) /630092, Новосибирск-92, пр. Карла Маркса, 20, т. 46-50-01,46-29-87 /3.1а,б;4;6 /
269 /ЛГ0010, 000472 /№270 /06.12.96 //06.12.99 /000 «Техническая испытательная лаборатория» /630092, Новосибирск-92, пр. Карла Маркса, 20, корп.7, т. 46-29-87 /1.2а;2.2б; 3.3б, г; 3.9б /
270 /ЛГ 0007, 000317 /№271 /06.12.96 /06.12.99 /АООТ «Центральное научно-производственное объединение «Каскад» (ЦНПО «Каскад») /125047, Москва, 1-я Брестская ул., 35, т. 251-7077, 250-3887 /3.3-3.6а-е; 3.9а-е; 5а, б, д, е /
271 /ЛГ0010, 000474 /№272 /10.12.96 /10.12.99 /ЗАО «Гарант-2К» /Москва, пр. Мира, 101 Б, оф. 20, т. 216-6805 /2а, б, г, д, е; 3а-в, е, ж; 4 /
272 /ЛГ0010, 000475 /№273 /10.12.96 /10.12.99 /Специальное конструкторское бюро института радиотехники и электроники Российской Академии наук (СКБ ИРЭ РАН) (РАН) /14П20.Фрязино Московской обл., пл. Введенского, 1,т. (095)526-9233 /2а, б, в, г; 3.1-3.2а-в; 3.3-3.7а-е; 3.8-3.9а-в; 5а-в /
273 /ЛГ0010, 000476 /№274 /10.12.96 /10.12.99 /ТОО «Лимб-СП» /141120, Фрязино Московской обл., ул. Октябрьская, 10, т. (095) 526-9233 /3.1-3.2а-в;3.3-3.9а-е; 5а-в /
274 /ЛГ0010, 000477 /№275 /19.12.96 /19.12.99 /ЗАО «Фирма «АйТи». Информационные технологии» /117218, Москва, а/я 116, «Фирма «АйТи». Информационные технологии», т. 127-9010, 127-9012 /2;3;4;5 /
275 /ЛГ0010, 000478 /№276 /23.12.96 /2Э.12.99 /000 «Экспресс-Сервис» /195027, Санкт-Петербург, ул. Тарасова, 8/7, кв.54, т. 248-0210, 227-0297 /2;3;4 /

Продолжение приложения 3

№ п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки

276 /ЛГ0010, 000479 /№277 /24.12.96 /24.12.99 /ГП 20 Центральный проектный институт Министерства обороны Российской Федерации (20 ЦПИ МО) /129085, Москва, пр. Мира, 101-В, т. 282-7444, 215-8419 /5а-в,д,е /
277 /ЛГ0010, 000480 /№278 /25.12.96 /25.12.99 /Производственный кооператив «Сигнал» /162622, Вологодская обл., Череповец, пр. Победы, 61, т.25-4873 /2; 3.3-3.9а-»; 4 /
278 /ЛГ0010, 000481 /№279 /26.12.96 /26.12.99 /ЗАО «Европеум-Щит» /123242, Москва, ул. Большая Грузинская, 14, комн. правления, т. 203-4435 /2; 3.4-3.5а, б; 3.8а, б; 4; 5 /
279 /ЛГ0010, 000482 /№280 /30.12.96 /30.12.99 /000 «Охранное агентство «Аргус» /103055, Москва, 2-й Вышеславцев пер., 17, т.973-3673 /2;3.1а-е; 3.3-3.6а-е; 3.8-3.9а-е /
280 /ЛГ0010, 000483 /№281 /08.01.97 /08.01.2000 /Главное управление Центрального банка РФ по Кировской области /610601, Киров, ул. Дрелевского, 27,т.65-3201,62-2081 /2; 3.4-3.6а-е; 3.9 /
281 /ЛГ0010, 000484 /№282 /08.01.97 /08.01.2000 /000 «Курганская региональная служба безопасности «Стрелец» /640002, Курган, ул. К. Мяготина, 175,т.7-0497,7-3256 /2в-е; 3а-д; 4 /
282 /ЛГ0010, 000485 /№283 /08.01.97 /08.01.2000 /000 «Центр технической защиты информации» /620078, Екатеринбург, ул. Студенческая,51, т. 74-8005, 74-8007 /2; 3.3-3.9а-е /
283 /ЛГ0010, 000486 /№284 /08.01.97 /08.01.2000 /АОЗТ «НИИИТ—

радиотехнические системы» /454048. Челябинск, ул. Витебская, 4, т. 34-79-84 /2; 3а-е;4 /
284 /ЛГ0010, 000487 /№285 /09.01.97 /09.01.2000 /ЗАО «Компания «СТРИМ» /111538, Москва, ул. Вешняковская, 27, корп. 2, пом. правления, т. 187-2465 /2; 3а-е; 4; 5а-в /
285 /ЛГ0010, 000488 /№286 /09.01.97 /09.01.2000 /ЗАО «АКАРА» /132022, Москва, Звенигородское ш., 9, т. 256-2397 /2; 3а-е; 4; 5а-в /
286 /ЛГ0010, 000489 /№287 /16.01.97 /16.01.2000 /ГП «Производственное объединение «Старт» (Минатом России) /440901, Заречный Пензенской обл., т. 69-2753, 69-2755 /2; 3.1-3.2а-в; 3.3-3.6а-г; 3.7-3.9а-в; 4; 5 /
287 /ЛГ0010, 000490 /№288 /16.01.97 /16.01.2000 /АООТ «Научно-технический центр «РАТЭК» /193224, Санкт-Петербург, а/я 26, Т.(812)587-5397 /2; 3; 4; 5а-в /
288 /ЛГ0010, 000491 /№289 /24.01.97 /24.01.2000 /ОАО «ИПРОМАШПРОМ» (Минэкономики России) /103473, Москва, Суворовская пл., 1, т. 281-2305/5д,е /
Продолжение приложения 3
№ п/п /Сери», номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки
289 /ЛГ0010, 000492 /№290 /24.01.97 /24.01.2000 /ЗАО «Радиус». Технические средства безопасности» /117334, Москва, Ленинский пр., 41/2,т. 135-3394 /2; 3.3-3.9а-е; 4; 5а-в /
290 /ЛГ0010, 000493 /№291 /24.01.97 /24.01.2000 /Конструкторское бюро машиностроения (Минэкономики России) /140402, Коломна Московской обл., Окский пр., 42, т. 3-40-52 /2; 3а-е; 4 /
291 /ЛГ0010, 000494 /№292 /30.01.97 /30.01.2000 /ООО «ПАЛАНГ» /103489, Москва, Зеленоград, завод «Стелла», т.535-1490 /2; 3а-в /
292 /ЛГ0010, 000495 /№293 /30.01.97 /30.01.2000 /ЗАО «Комита» /195272, Санкт-Петербург, Малоохтинский пр.,55, т.(812)528-3466,528-6467 /3.1-3.4г-е;3.6г-е; 3.9г-е /
293 /ЛГ0010, 000498 /№294 /30.01.97 /30.01.2000 /ТОО «Иста-системс» /197342, Санкт-Петербург, ул. Торжковская, д.4, т.(812)296-3548 /3.3-3.9а-ж /
294 /ЛГ0010, 000499 /№295 /07.02.97 /07.02.2000 /ООО «АКРАС ИПП» /107066, Москва, ул. Ольховская, 45, кв. 221,т.261-8816 /3.3-3.9а-е /
295 /ЛГ0010, 000500 /№296 /07.02.97 /07.02.2000 /Институт криптографии, связи и информатики Академии федеральной службы безопасности РФ /107602, Москва, Мичуринский пр., 70, т. 931-0609,931-0527 /6 /-
296 /ЛГ 0007, 000301 /№297 /07.02.97 /07.02.2000 /Дочернее предприятие ОАО «Газпроектинжиниринг» /394028, Воронеж, Ленинский пр., 119, т. 22-45-01 /5д,е /
297 /ЛГ 0007, 000302 /№298 /07.02.97 /07.02.2000 /ЗАО «РФК» /107076, Москва, Преображенская пл., 6/68, стр.3, т. 964-2519 /3а,г-е /
298 /ЛГ 0007, 000303 /№299 /10.02.97 /10.02.2000 /ООО «Компания «Демос» /113035, Москва, Овчинниковская наб., 6/1, т. 956-6272 /1.2; 2; 3; 4; 5а-в /
299 /ЛГ 0007, 000304 /№300 /20.02.97 /20.02.2000 /ЗАО «Банковский производственный центр» /103051, Москва, ул. Трубная, 25, стр.1,т.926-5981,926-5982 /3.3-3.9а, б, г, д /
300 /ЛГ 0007, 000305 /№301 /20.02.97 /20.02.2000 /ОАО «Главный информационно-вычислительный центр Москвы» /107078, Москва, ул. Каланчевская, 27, т. 208-0745 /3.1-3.9г,д,е /
301 /ЛГ0007, 000306 /№302 /20.02.97 /20.02.2000 /АООТ «МГПИ» /117313,

Москва, Старокалужское ш.,62,т.128-9910 /2-.S /
302 /ЛГ0001, 000012 /№303 /14.11.97 /14.11.2000 /000 «Ай Си Эс» /107082, Москва, ул. Фридриха Энгельса, 67,т.913-9981 /2; 3; 4; 5а, б /
303 /ЛГ 0007, 000308 /№304 /26.02.97 /26.02.2000 /ЗАО «Документальные системы—МФД» /123242, Москва, а/я 26, т.252-0753,252-5102/1.2;2;3 /

**Продолжение приложения 3**

№ П/П /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки

304 /ЛГ 0007, 000309 /№305 /26.02.97 /26.02.2000 /000 «САЛД» /196015, Санкт-Петербург, ул. Благодатная, 34, Т.(812)298-8624 /3.1-3.4г-ж; 3.6-3.9г-ж /
305 /ЛГ 0007, 000311 /№306 /14.03.97 /14.03.2000 /Войсковая часть 2599 (ФПС России) /117437, Москва, ул. Островитянова, 15-А, т.330-9386,330-9243 /2.2а, б, г, д, с; 3.4-3.8; 4; 5а, б /
306 /ЛГ0019, 000928 /№307 /14.03.97 /14.03.2000 /ЗАО «Научно-производственное объединение «Криптон» /123424, Москва, Волоколамское ш., 90, т. 491-8789 /3а, в. г, д, е, ж; 1.2 /Изменено
307 /ЛГ 0007, 000313 /№308 /20.03.97 /20.03.2000 /Научно-производственная фирма «Информационная техника и технологии» (ИНФОТЕХ) /109004, Москва, ул. Верхняя Радищевская, 7, т. 915-7706 /2; 3а-е; 4 /
308 /ЛГ 0007, 000314 /№309 /20.03.97 /20.03.2000 /ТОО «Экономические программы» /109180, Москва, 1-й Голутвинский пер., 3-2, т. 238-3520 /2; 3а-е; 4; 5 /
309 /ЛГ0007, 000315 /№310 /25.03.97 /25.03.2000 /ТОО «Научно-производственное товарищество «Пролог» /150000, Ярославль, ул. Свободы, 46/19, ЦОС, а/я 942, т. (0852) 30- 24-04 /2; 3.3-3.9;4 /
310 /ЛГ 0007, 000316 /№311 /25.03.97 /25.03.2000 /ГУП «Аттестационный центр Желдоринформзащита МПС РФ» (МПС) /107174, Москва, ул. Новая Басманная, 2, т. 256-2397, 262-2716 /1.2;2;3;4;5а-в /
311 /ЛГ 0007, 000318 /№312 /25.03.97 /25.03.2000 /Управление внутренних дел Пензенской области (МВД) /440009, Пенза,ул.Злобина,52, т. (841-2) 69-93-93, 69-96-67, 66-43-40 /2б-е; 3.3а-в; 3.4-3.6а-в; 3.8-3.9а-в; 4 /
312 /ЛГ 0007, 000319 /№313 /03.04.97 /03.04.2000 /ЗАО «Управление перспективных технологий» /115409, Москва, Каширское ш., 44, корп. 2, т.323-3910,323-3710 /2; 3.3-3.9а-е; 4; 5 /
313 /ЛГ 0007, 000320 /№314 /03.04.97 /03.04.2000 /ЗАО «БАГс» /390046, Рязань, а/я № 19, т. 93-04-00,53-47-00 /2а, б, г, д, е; 3а-е; 4 /
314 /ЛГ 0007, 000321 /№315 /04.04.97 /04.04.2000 /ОАО «Холдинговая компания «ЭЛЕКТРОЗАВОД» /105023, Москва, ул. Электрозаводская,21, т.968-1098,962-1652 /1.2;2;3;4;5а-в /
315 /ЛГ 0007, 000323 /№316 /10.04.97 /10.04.2000 /ЗАО «БАРЬЕР-1» /123557, Москва, Пресненский вал, 28, стр.1, комн. правления, т.190-7772 /1.2;2;3;4;5а-в /
316 /ЛГ 0007, 000324 /№317 /10.04.97 /10.04.2000 /ОАО «КБ ИМПУЛЬС» /125083, Москва, ул. 8 Марта, 10-12, т. 212-9940,264-9601- /3а-е /

Продолжение приложения 3

№ п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки

317 /ЛГ 0007, 000326 /№318 /15.04.97 /15.04.2000 /ЗАО «ЭЛЕКТРЕТ» /344090, Ростов-на-Дону, пр. Стачки, 194, оф. 715, т. 28-52-00 /2; 3.1; 3.3-3.9; 4 /
318 /ЛГ0007, 000327 /№319 /15.04.97 /15.04.2000 /000 «Монтажно-

технологическое управление «Телеком-С» /355044, Ставрополь, пр. Кулакова, 5-1 Г,т.76-12-20 /2; 3.3-3.9; 4 /

319 /ЛГ0007, 000328 /№320 /15.04.97 /15.04.2000 /ГП «Всероссийский научно-исследовательский институт физико-технических и радиотехнических измерений» (ВНИИФТРИ) (Госстандарт России) /141570, Московская обл., Солнечногорский р-н, п/о Менделеево, т. 535-2401 1 /1.2а-в;2;3а,в;4 /

320 /ЛГ0007, 000329 /№321 /21.04.97 /21.04.2000 /АООТ «Амурская Эра» /681000, Хабаровский край, Комсомольск-на-Амуре, ул. Аллея Труда, 8/6, т. 4-51-10, 4-31-Й) /1.2а,в;2в-е; 3.2а, в; 4 /

321 /ЛГ0004, 000160 /№322 /25.4.97 /4.9.2001 /ГП «Центральный научно-исследовательский институт связи» (ЦНИИС) (Госкомсвязи России) /111141, Москва, 1-й проезд Перова поля, 8, т. 306-3278, 368-9181 /1.2; 2.26; 36, г-ж; 4; 56 /Изменено

322 /ЛГ 0007, 000331 /№323 /30.04.97 /30.04.2000 /000 «Технолоджи» /113162, Москва, ул. Татищева, 3, стр.1, т. 958-5103,958-5114 /2е /

323 /ЛГ 0007, 000332 /№324 /30.04.97 /30.04.2000 /ЗАО «Специализированное агентство информации и безопасности «ТЕХКОМ» /109507, Москва, Самаркандский б-р, 15, корп.4,т.275-058) /2; 3.3-3.6; 3.8-3.9 /

324 /ЛГ 0007, 000333 /№325 /30.04.97 /30.04.2000 /Государственное научно-производственное объединение «Циклон-Тест» (Минэкономики России) /141120,Фрязино Московской обл., Заводской проезд, 4,т. 526-9173, 465-8608 /1.2а-е;2.2;3а-в; 4 /

235 /ЛГ0007, 000334 /№326 /05.05.97 /05.05.2000 /Военный институт радиоэлектроники ВИРЭ (Минобороны России) /394020, Воронеж, ул. Краснознаменная, 153, т. 36-92-93 (доб. 5-01), 36-25-57 /2б,д,е; 3.3-3.7а, в; 3.9а, в; 4; 6 /

326 /ЛГ 0007, 000335 /№327 /05.05.97 /05.05.2000 /ИЧП Казакова «АНИРКА» /127549, Москва, ул. Мурановская, 6-160, т.972-1179 /3.3а, б, в /

327 /ЛГ 0007, 000336 /№328 /06.05.97 /06.05.2000 /000 «Детективное предприятие «РОСТИНЕКСДЕТЕКТИВ» /Ростов-на-Дону, пер. Братский, 47, т. (8632) 66-84-41 /2;3.4-3.9а-в;4 /

328 /ЛГ0019, 000939 /№329 /21.05.97 /21.05.2000 /ОАО «Информационно-инженерная фирма «КИБ» /129085, Москва, пр. Мира, 81-227,т.928-7059 /3г, д, е /Продлено и изменено

329 /ЛГ 0007, 000340 /№330 /29.05.97 /29.05.2000 /ЗАО «Х-Ринг Техно» /117259, Москва, ул. Большая Черемушкинская, 25, т. 123-7305, 125-9735 /3.2-3.6а-в; 3.8-3.9а-в/

Продолжение приложения 3

№ п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки

330 /ЛГ 0007, 000341 /№331 /04.06.97 /04.06.2000 /Тамбовский государственный научно-исследовательский институт радиотехники «Эфир» (Минэкономики России) /392000,Тамбов, ул. Коммунальная, 25, т. 22-50-72, 22-50-96 /2; 3; 4; 5а-в /

331 /ЛГ 0007, 000342 /№332 /04.06.97 /04.06.2000 /Центр компьютерной безопасности Министерства обороны Российской Федерации (ЦКБ МО) (Минобороны России) /103106, Москва, К-160, ул.Знаменка, 19, т.296-7817, 293-3956 /1;2;3 /

332 /ЛГ0007, 000343 /№333 /04.06.97 /04.06.2000 /АОЗТ «ПРОМИНФОРМ» /614088, Пермь, ул. Свиязева, 28«б»-47, т. (3422) 34-35-94, "34-35-08 /3.1-3.9а-б /

333 /ЛГ 0007, 000344 /№334 /10.06.97 /10.06.2000 /АООТ «Измеритель»

/113191, Москва, Холодильный пер., 1, т. 954-4939 /1.2г,д,е;3а,г,д,е /
334 /ЛГ 0007, 000345 /№335 /10.06.97 /10.06.2000 /ЗАО «МТТ КОНТРОЛ» /125047, Москва, ул. Готвальда, 8/26, т. 237-5047 /3г-е /
335 /ЛГ 0007, 000347 /№336 /17.06.97 /17.06.2000 /Государственное унитарное предприятие Специализированный центр программных систем «СПЕКТР» (Минэкономики России) /197342, Санкт-Петербург, ул. Кантемировская, 10, Т.(812)245-3693 /1.2; 2; 3:4; б /Продлено и изменено
336 /ЛГ 0007, 000348 /№337 /17.06.97 /17.06.2000 /ЗАО «Научно-производственное объединение «Опыт» (НПО «ОПЫТ») /125319, Москва, Авиационный пер., 5, т. 157-9841 /3а-с; 5а-в /
337 /ЛГ 0007, 000349 /№338 /17.06.97 /17.06.2000 /ЗАО «Научно-производственное объединение «Кибернетика» /117420, Москва, ул. Профсоюзная, 78, т. 120-3410 /1.2г-ж; 2а; 3.1-3.4г-ж; 3.7г-ж; 3.9г-ж /
338 /ЛГ0019, 000901 /№339 /17.06.97 /17.06.2000 /ОАО «Иркутское авиационное производственное объединение» /664020, Иркутск, ул. Новаторов, 3, т. 32-29-02 /1.2г-ж;2а; 3.1-3.4г-ж; 3.7г-ж; 3.9г-ж /
339 /ЛГ0001, 000001 /№340 /11.02.98 /11.02.2001 /ОАО «ОПТИМА» /107082, Москва, Рубцовская наб., 3, стр.1, т. 263-9946 /1.2;2;3;4;5 /Продлено и изменено
340 /ЛГ0019, 000903 /№341 /25.06.97 /25.06.2000 /Некоммерческая организация «Секция «Информбезопасность» (РИА) /107005, Москва, ул. 2-я Бауманская, 5, т. 263-6792 /1.1г-ж;2а-в; 3.1-3.6; 3.9; 4 /
341 /ЛГ0019, 000904 /№342 /03.07.97 /03.07.2000 /ЗАО «Урал-Сканер» /620085,Екатеринбург, ул. Ферганская, 16, т. (3432) 62-39-01,62-39-04 /2;3;4 /
342 /ЛГ0019, 000905 /№343 /08.07.97 /08.07.2000 /ООО фирма «ВЕНАВИТ» /117049, Москва, Крымский вал, 8, т.263-1957/3а;5е /
Продолжение приложения 3
№ п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки
343 /ЛГ0019, 000906 /№344 /08.07.97 /08.07.2000 /ООО «ФИТА» /180007, Псков, ул. Розы Люксембург, 13, т. (811-2) 46-77-49 /2.2а; 3; 5а, б /
344 /ЛГ0019, 000907 /№345 /10.07.97 /10.07.2000 /Общественное объединение «Ассоциация документальной электросвязи» (АДЭ) /111024, Москва, ул. Авиамоторная, 8а, т. 273-4883,362-6413 /6 /
345 /ЛГ0019, 000908 /№346 /15.07.97 /15.07.2000 /ТОО «Научно-техническая коммерческая фирма «ИНГА» /197342, Санкт-Петербург, ул. Сердобольская,64, т.230-0885 /1.2а-в;2;4;3а-в; 5а-в /
346 /ЛГ0019, 000909 /№347 /15.07.97 /15.07.2000 /Северо-Западный инновационный центр при Санкт-Петербургском государственном электротехническом университете (Минобразования России) /197376, Санкт-Петербург, ул. Профессора Попова, 5, т. 234-2917 f /3.1-3.6а /
347 /ЛГ0019, 000910 /№348 /15.07.97 /15.07.2000 /ООО «Частное охранное предприятие «АДЪЮТАНТ» /123022, Москва, Звенигородское ш., 9, т. 256-8382 /2; 3.1а-е; 3.3-3.9а-е /
348 /ЛГ0019, 000912 /№349 /22.07.97 /22.07.2000 /ГУП «Научно-технический центр «Атлас» (НТЦ «АТЛАС») (ФАПСИ) /127018, Москва, ул. Образцова, 38, т. 289-2222 /1а-е;2;3;4;5а-в /
349 /ЛГ0019, 000941 /№350 /01.10.97 /01.10.2000 /Управление внутренних дел Красноярского края (МВД) /660017, Красноярск, ул. Дзержинского, 18, т. (391-2) 27-62-25 /2б-е; 3.3-3.6 а-в; 3.8-3.9а-в; 4 /
350 /ЛГ0019, 000915 /№351 /23.07.97 /23.07.2000 /Научно-

исследовательский институт импульсной техники (НИИИТ) (Минатом России) /115304, Москва, М-304, НИИИТ, т. 321-3501, 321-4474 /1.2а-в;2а-в; 3а-в; 4 /

351 /ЛГ0019, 000916 /№352 /24.07.97 /24.07.2000 /ТОО «Научно-исследовательский центр «ФОРС» /443011, Самара, ул. Советской Армии, 217, т. (846-2) 99-67-68 /3.1а-е; 3.3-3.9а-е; 5 /

352 /ЛГ0019, 000917 /№353 /07.08.97 /07.08.2000 /ПО «Уральский оптико-механический завод» (Минэкономики России) /620100, Екатеринбург, ул. Восточная, 33 «Б», т. (3432) 24-80-52 /2; 3.3-3.7; 3.9; 4 /

353 /ЛГ0019, 000918 /№354 /07.08.97 /07.08.2000 /ООО «ЕЛЕКТРО» /344012,Ростов-на-Дону, пр. Ворошиловский, 46, т. 666-574 /3.3-3.6а, б, г-е; 3.7г-е; 3.8-3.9а, б, г-е /

354 /ЛГ0019, 000922 /№355 /13.08.97 /13.08.2000 /ЗАО «КДС—Технический центр» /123299, Москва, Шелепихинская наб., 18, т. 259-8818,259-7936 /3.8-3.9а-в /

355 /ЛГ0019, 000923 /№356 /13.08.97 /13.08.2000 /ООО «Московская информационная сеть» /103104, Москва, Тверской б-р, 7/2, К-104, а/я 103, т. 203-7445 /3в-е /

Продолжение приложения 3

№ п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки

356 /ЛГ 0003, 000104 /№357 /28.08.97 /28.08.2000 /ООО «Научно-производственная фирма «Новь» /614000, Пермь, ул. Краснова, 26, т.(3422)348-956 /2.1е; 3.3-3.9а /Замена бланка (переименование)

357 /ЛГ0019, 000925 /№358 /28.08.97 /28.08.2000 /ГП «Научно-исследовательский институт информационных технологий» (Минэкономики России) /170000, Тверь, ул. Володарского, 3, т. (0822) 33-27-01, 33-29-83 /2а, г-е; 3а-г; 4 /

358 /ЛГ0019, 000926 /№359 /28.08.97 /28.08.2000 /ООО «Координатор» /445005,Тольятти, ул. Гидротехническая, 37, т. 29-22-34 /3.3-3.5а-в; 3.8а-в /

359 /ЛГ0019, 000927 /№360 /28.08.97 /28.08.2000 /ЗАО «Автоматизированные Банковские Технологии» /103031, Москва, ул. Пушечная, 5, т. 928-7059, 921-4380 /3г-е; 3.2-3.6 а-е; 3.7г-е; 3.8-3.9а-е /

360 /ЛГ0019, 000930 /№361 /17.09.97 /17.09.2000 /Санкт-Петербургский государственный технический университет (Минобразования России) /195251, Санкт-Петербург, ул. Политехническая, 29, т. (812) 552-6489, 552-6252 /1.2;2а,б;3.1; 3.7; 5а; 6 /

361 /ЛГ0019, 000932 /№362 /12.09.97 /12.09.2000 /ООО «СПУРТ Лтд.» /113405, Москва, Варшавское ш., 125,т.319-6118 /2; 3а-е;4 /

362 /ЛГ0019, 000933 /№363 /17.09.97 /17.09.2000 /ОАО «Радиофизика» /123364, Москва, ул. Героев Панфиловцев, 10, т. 493-4048 /2.1а-г;3а,б,г-ж /

363 /ЛГ0019, 000934 /№364 /17.09.97 /17.09.2000 /ЗАО «СПЕЦСВЯЗЬСЕРВИС» /117261, Москва, Ленинский пр., 72/2, т. 974-6035 (39) /1.2а-в;2;3а-в; 5а-в /

364 /ЛГ0019, 000935 /№365 /17.09.97 /17.09.2000 /ООО«ГЕЛИКОР» /123100, Москва, ул. Анатолия Живова, 8, оф.1, т. 259-8575 /2; 3а-е;4 /

365 /ЛГ0019, 000936 /№366 /18.09.97 /18.09.2000 /ЗАО «АВИКОМП СЕРВИСЕЗ» /117607, Москва, Мичуринский пр., 31, корп.1, т. 436-0145 /3г-е; 5а /

366 /ЛГ0019, 000937 /№367 /29.09.97 /29.09.2000 /Некоммерческое партнерство «Приморский региональный аналитический центр» (ПРАЦ)

(Администрация Приморского края) /690010, Владивосток, ул. Светланская,22, т. 260-736,217-475 /1.2а-е;2;3;4;5 /
367 /ЛГ0019, 000938 /№368 /29.09.97 /29.09.2000 /ТОО «РЕНОМ» /117602, Москва, ул. Академика Анохина,12,т.430-9225 /3.2-3.3а, б; 3.8-3.9а, б /
368 /ЛГ0019, 000940 /№369 /01.10.97 /01.10.2000 /ТОО «Фирма «ТИАРА» /127490, Москва, Юрловский проезд, 1, т. 404-4944, 404-7745 /3.1-3.9а-ж;4 /
369 /ЛГ0019, 000945 /№370 /07.10.97 /07.10.2000 /АООТ «Ракетно-космическая корпорация «Энергия» имени С.П.Королева» /141070, Королев Московской обл., ул. Ленина, 4а, т. 513-7506, 513-7248 /2; 4 /
Продолжение приложения 3
№ п/п /Серия, номер бланка/Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки
370 /ЛГ0019, 000946 /№371 /07.10.97 /07.10.2000 /ООО «Проектно-коммерческая фирма «Безопасность» /170000, Тверь, ул. Крылова, 14, т. 55-1905 /3.3а-е /
371 /ЛГ0019, 000949 /№372 /17.10.97 /17.10.2000 /ЗАО «ЭКА» /141080, Юбилейный Московской обл., в/ч 73790-0, т. 519-8704 /2; 3а-е; 4; 5а /
372 /ЛГ0001, 000006 /№373 /05.11.97 /05.11.2000 /ЗАО «ЛОТОС СИСТЕМЫ» /680000, Хабаровск, ул. Серышева, 22, т. (412-2) 22-33-67 /1.2; 2; 3.3-3.9; 4; 5а-в /
373 /ЛГ0001, 000009 /№374 /06.11.97 /06.11.2000 /АОЗТ «КОМТРАНССТРОЙ» /394000, Воронеж, ул. Кольцовская, 7/27, Т.(0732)55-1259. /3.3-3.6а; 3.8-3.9а; 5д,е /
374 /ЛГ0001, 000011 /№375 /14.11.97 /14.11.2000 /ОАО «Электросвязь»— Кемеровская городская телефонная сеть» /650099,Кемерово, ул. Красноармейская, 99, т. 25-14-4 /2.1б,е;33-3.4а /
375 /ЛГ0001, 000014 /№376 /20.11.97 /20.11.2000 /ЗАО «Научно-технический центр «Современные системы и сети» /111250, Москва, наб. Академика Туполева, 15, т. 202-2517, 267-2572 /2; 3.3-3.9а-с; 4; 5а-в /
376 /ЛГ0001, 000015 /№377 /20.11.97 /20.11.2000 /ООО «Северный Радиус» /194037, Санкт-Петербург, ул.Заповедная, 2, Т.(812)269-9058 /3.1г-е;3.7г-с; 3.2-3.6а-е; 3.8-3.9а-е /
377 /ЛГ0001, 000016 /№378 /20.11.97 /20.11.2000 /ГП «15-й Центральный научно-исследовательский испытательный институт Министерства обороны Российской Федерации» (15 ЦНИИ МО) (Минобороны России) /143430, Московская обл., Красногорский р-н, пос. Нахабино-2, т.561-2185,560-3126 /2а-е; 4 /
378 /ЛГ0001, 000018 /№379 /26.11.97 /26.11.2000 /ООО «АРТИС КОМПАНИ» /107850, Москва, ул. Просторная, 7,т. 168-2042 /3.1г-е;3.7г-е; 3.2-3.6а-е; 3.8-3.9а-е /
379 /ЛГ0001, , 000019 /№380 /26.11.97 /26.11.2000 /ТОО «ПРИБОРМОНТАЖ» /Астрахань, ул. Максима Горького,25,т.22-45-15 /3.3а-е /
380 /ЛГ0001, 000020 /№381 /28.11.97 /28.11.2000 /ТОО «Научно-производственное предприятие «РЕЛЭКС» /394006, Воронеж, ул. 20-летия Октября, 119,т.71-17-11 /3г-ж; 5а-в /
381 /ЛГ0001, 00021 /№382 /28.11.97 /28.11.2000 /ЗАО «Центр информационных технологий «КАМИ» /123363, Москва, ул. Героев Панфиловцев, 10, т. 493-4048 /2;3;4;5 /
382 /ЛГ0001, 000022 /№383 /04.12.97 /04.12.2000 /ГП «Воронежский научно-исследовательский институт связи» (Минэкономики России) /Воронеж, ул. Плехановская, 14, т. 52-19-40, 52-12-59 /3а /
Продолжение приложения 3

№ п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки

383 /ЛГ0001, 00023 /№384 /04.12.97 /04.12.2000 /ЗАО «Концерн ВНИИНС» /113149, Москва, ул. Сивашская, 4-2, т. 119-6842 /3; 5а-в /

384 /ЛГ0001, 000024 /№385 /04.12.97 /04.12.2000 /ТОО «Научно-техническое предприятие «ЭОС» /440026, Пенза, ул. Советская, 9, т. 69-09-31 /3а-ж /

385 /ЛГ0001, 000026 /№386 /19.12.97 /19.12.2000 /ОАО «Псковский завод автоматических телефонных станций» /180004, Псков, ул. Яна Фабрициуса, 10, т. 2-31 -62 /2;3а-е /

386 /ЛГ0001, 000027 /№387 /19.12.97 /19.12.2000 /ООО «Особое конструкторское бюро САПР» (ОКБ САПР) /113114, Москва, 2-й Кожевнический пер., 4/6, т. 235-1606 /3.2-3.6; 3.8- 3.9; 3.1а,г-е;3.7а, г-е /

387 /ЛГ0001, 000028 /№388 /19.12.97 /19.12.2000 /Отдел вневедомственной охраны при УВД г. Череповца (МВД России) /162627, Череповец Вологодской обл., б-р Доменщиков, 34,т.27-03-95,27-69-11 /2б-е; 3.3-3.6 а-в; 3.8-3.9а-в; 4 /

388 /ЛГ0001, 000029 /№389 /19.12.97 /19.12.2000 /Управление внутренних дел Тверской области (МВД России) /170005, Тверь, пл. Мира, 70/1, т. 31-31-33,31-64-64 /2б-е; 3.3-3.6 а-в; 3.8-3.9ав; 4 /

389 /ЛГ0001, 000031 /№391 /25.12.97 /25.12.2000 /Московский земельный комитет (Правительство Москвы) /113054, Москва, ул. Бахрушина, 20, т. 959-1984 /2; 3.4а-д; 3.6а-д; 3.9а-д;4 /

390 /ЛГ0001, 00032 /№392 /25.12.97 /25.12.2000 /ЗАО «Научно-производственное предприятие «РАДИАНТ» /107066, Москва, ул. Новая Басманная, 20, т. 263-9467 /3а-в /

391 /ЛГ0001, 000033 /№393 /25.12.97 /25.12.2000 /ООО «Департамент СТС защиты информации» /194175, Санкт-Петербург, Выборгская наб., 7, т. 542-8650 /2.1б,г,е**) /

392 /ЛГ0001, 000034 /№394 /25.12.97 /25.12.2000 /ЗАО «Контроль-Сервис» /129278, Москва, Рижский проезд, 5, РЭП-2, т. 283-0382 /2а-е; 3.2-3.6 а-е; 3.8-3.9 а-е **) /

393 /ЛГ0001, 000035 /№395 /25.12.97 /25.12.2000 /ООО «МОНТАЖАВТОМАТИКА» /603122, Нижний Новгород, ул. Козицкого, 4, т. 40-76-05 /3.3а-е /

394 /ЛГ0017, 000832 /№396 /29.07.98 /29.17.2001 /ОАО «ICL—КПО ВС» /420029, Казань, ул. Сибирский тракт, 34, т. (8432) 75-24-43, 75-19-32,76-26-03 /1.2; 2; 3:4; 5; 6 /Продлено и изменено

395 /ЛГ0001, 000037 /№397 /29.12.97 /29.12.2000 /ЗАО «Энерго-Ч» /125299, Москва, ул. Космонавта Волкова, 12, оф.802, т. 156-8957 /3.1г-е;3.7г-е; 3.2-3.6а-е; 3.8-3.9а-е /

396 /ЛГ0001, 000038 /№398 /06.01.98 /06.01.2001 /ЗАО «Лаборатория Касперского» /123363, Москва, ул. Героев Панфиловцев, 10, т. 948-4331,495-0300 /3г, д, е /

397 /ЛГ0001, 000039/№399 /06.01.98 /06.01.2001 /ТОО «ФАКТОР» /123557, Москва, Пресненский вал, 14, т. 253-5620/2; 3а-е **) /

Продолжение приложения 3

№ п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки

398 /ЛГ0001, 000040 /№400 /06.01.98 /06.01.2001 /ГУП «Отраслевой аттестационный научно-технический Центр безопасности информации и режима» (Минэкономики России) /103104, Москва, Тверской б-р, 7/2, т. 291-8714 /2;3;4 /

399 /ЛГ0001, 000041 /№401 /22.01.98 /22.01.2001 /ЗАО «МТЕ» /101000, Москва, Центр, а/я 525, т. 299-4051,299-4830 /2а-в;3.1;3.7; 5а-в /
400 /ЛГ0001, 000042 /№402 /22.01.98 /22.01.2001 /ООО «Научно-технический центр ЕВРААС»/109260, Москва, ул. Автозаводская, 19,к.3, оф. 34, т. 274-6019 /3.1г-е;3.7г-е; 3.2-3.6а-е; 3.8-3.9а-е; /
401 /ЛГ0001, 000043 /№403 /22.01.98 /22.01.2001 /ТОО «Научно-производственная фирма «РАДИОСЕРВИС» /123260, Москва, ул. Катукова, 20, корп. 1, кв.108, <214-7бб2 /3.1г-е;3.7г-с; 3.2-3.6а-е; 3.8-3.9а-е; /
402 /ЛГ0001, 000044 /№404 /22.01.98 /22.01.2001 /ЗАО «Инициатива-93» /119121, Москва, 1-й Вражский пер., 4, стр.1, т. 247-3477 /2.1а-е;3.3-3.9а-в; 5 /
403 /ЛГ0001, 000045 /№405 /29.01.98 /29.01.2001 /Научно-исследовательский институт промышленного телевидения «Растр» (Минэкономики России) /173001, Новгород, ул. Большая Санкт-Петербургская, 39, т. 7-43-31 /36 /
404 /ЛГ0001, 000046 /№406 /29.01.98 /29.01.2001 /ЗАО «Камсан Электронные системы» /129090, Москва, ул. Троицкая, 15, т. 284-5216 /2;3.Iа-е; 3.1-3.9а-е;4;5 /
405 /ЛГ0008, 000398 /№407 /16.06.98 /16.06.2001 /ТОО «Наладочно-производственное предприятие «КАСКОД» /107005, Москва, 2-я Бауманская ул., 9/23, корп. 18, т. 978-5883, 978-5713 /1.2а-е; 2; 3.3-3.9а-е; 5 /
406 /ЛГ0001, 000008 /№408 /11.02.98 /11.02.2001 /ООО «ТЕРОКС» /Хабаровск, ул. Герасимова, 38, корп.47,т.35-9103, /3.3-3.6а-е;3 .8-3.9а-е /
407 /ЛГ0001, 000049 /№409 /11.02.98 /11.02.2001 /АОЗТ «Центр технологий безопасности» /620086, Екатеринбург, ул. Посадская, 21, т. 23-0030 /3.3-3.6а, б, г, д 3.8-3.9а, б, г, д /
408 /ЛГ0001, 000050 /№410 /11.02.98 /11.02.2001 /ЗАО «КРОК инкорпорейтед» /103051, Москва, Большой Каретный пер., 22, стр.1, т.200-1696 /3.1г-е; 3.2-3.6а-е; 3.8-3.9а-е; 3.7г-е /
409 /ЛГ0008, 000351 /№411 /17.02.98 /17.02.2001 /ООО «Специализированный деловой центр по информационной безопасности и специальным техническим средствам» /196247, Санкт-Петербург, пл. Конституции, 2, т. 123-0781 /2; 3а-е; 4 /
410 /ЛГ 0008, 000352 /№412 /19.02.98 /19.02.2001 /ЗАО «ЛУКОЙЛ-ИНФОРМ»/101000, Москва, Сретенский б-р, 11, т. 927-4164, 927-4324 /2; 3.3-3.9а-е; 5 /

Продолжение приложения 3

№ п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки

411 /ЛГ 0008, 000353 /№413 /19.02.98 /19.02.2001 /ТОО «Объединение частных детективов «Агентство ДИСБИ» /Барнаул, Социалистический пр., 63, т. 24-4718, 24-4711 /2.1е,д /
412 /ЛГ0008, 000354 /№414 /24.02.98 /24.02.2001 /ЗАО «Рэйс-Коммуникейшн» /125080, Москва, Ленинградское ш., 5, корп.24, оф. 407, т. 785-0770, 158-4028 /3.3-3.7а, г, д, ж 3.9а, г, д, ж; 5а, б /
413 /ЛГ 0008, 000355 /№415 /24.02.98 /24.02.2001 /Центральный НИИ «Комета» (Минэкономики России) /109280, Москва, ул. Велозаводская,5,т.275-3340 /2; 3.3-3.6а-в; 3.8-3.9а-в;4 /
414 /ЛГ 0008, 000356 /№416 /24.02.98 /24.02.2001 /ООО «ЦЕРБЕР» /Подольск Московской обл., ул. Маштакова, 12, т.57-38-82,137-0308 /3.2-3.6а-е; 3.8-3.9а-е;3.1г-е; 3.7г-е /
415 /ЛГ 0008, 000357 /№417 /25.02.98 /25.02.2001 /ООО «Научно-

производственная фирма «ПЛИС-Лтд.» /107066, Москва, ул. Новая Басманная, 20, т?261-б981 /3а-в /

416 /ЛГ 0008, 000358 /№418 /04.03.98 /04.03.2001 /ЗАО «Спецзнак» " /117330, Москва, Ленинский пр., 53, т. 135-8704 /3.2-3.6а-е; 3.8-3.9а-е;3.1г-е; 3.7г-е /

417 /ЛГ 0008, 000359 /№419 /04.03.98 /04.03.2001 /ТОО «Интекгран-Сервис» /121357, Москва, ул. Артамонова, 11,т.146-1654 /3.2-3.6а-е; 3.8-3.9а-е;3.1г-е; 3.7г-е /

418 /ЛГ 0008, 000360 /№420 /17.03.98 /17.03.2001 /000 «К-Системс» /123363, Москва, ул. Героев Панфиловцев, 10А, т. 492-8512, 948-3650 /3.2-3.66; 3.8-3.96 /

419 /ЛГ 0008, 000361 /№421 /17.03.98 /17.03.2001 /Научно-исследовательский институт «Вычислительные технологии» (Минобразования России) /119435, Москва, Большой Саввинский пер., 14, т. 246-3043 /3.1-3.4г-е; 3.7г-е; 3.9г-е /

420 /ЛГ 0008, 000362 /№422 /17.03.98 /17.03.2001 /«Особое конструкторское бюро Московского энергетического института» (ОКБ МЭИ) (Минобразования России) /111250, Москва, ул. Красноказарменная, 14, т. 362-5652 /1.2а-е;2б;3а-в;4 /

421 /ЛГ 0008, 000364 /№423 /24.03.98 /24.03.2001 /ТОО «Научно-производственный центр «СОТИС» /141090, Юбилейный Московской обл., в/ч 73790,т.515-2560 /2; 3а-е; 4; 5а-в /

422 /ЛГ 0008, 000365 /№424 /24.03.98 /24.03.2001 /ЗАО «Информсвязь Холдинг» /117602, Москва, Олимпийская дер.. Мичуринский пр., 1, т. 437-5298,437-8613 /3.1г-е; 3.2-3.6а-е; 3.7г-е; 3.8-3.9а-е; 5а-в /

423 /ЛГ 0008, 000366/№425 /24.03.98 /24.03.2001 /Военно-инженерная академия им. В. Куйбышева (Минобороны России) /109028, Москва, Покровский б-р, 11,т.916-8373 /2; 3а-е /

Продолжение приложения 3

№ п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки

424 /ЛГ 0008, 000367 /№426 /24.03.98 /24.03.2001 /000 «Частное охранное предприятие «ВАРЯГ» /125284, Москва, Ленинградский пр., 33, корп.5, т. 378-3077 /2а-е; 3.1а-е; 3.3-3.9а-е; 4; 5а-в /

425 /ЛГ0008, 000368 /№427 /27.03.98 /27.03.2001 /Московское авиационное производственное объединение «МИГ» (Минэкономики России) /125040, Москва, 1 -и Боткинский проезд, 7,т.252-8770,252-8960 /2б-е; 3.4а-е; 3.5а-в; 3.6а-е; 3.1-3.3а,в; 3.7-3.9а, в; 4; 5д /

426 /ЛГ0008, 000370 /№428 /08.04.98 /08.04.2001 /000 «Фирма «АВТОЛИК» /111123, Москва, ул. 2-я Владимирская, 10, стр.1, т. 304-5565 /3.1г-е;3.7г-е; 3.2-З.ба-е; 3.8-3.9а-е /

427 /ЛГ0008, 000371 /№429 /08.04.98 /08.04.2001 /Министерство внутренних дел Республики Татарстан (МВД России) /420111, Казань, ул.Дзержинского, 19, т. (843-2) 64-33-40, 32-75-43 /2; 3.3-З.ба-в; 3.8-3.9а-в;4 /

428 /ЛГ0008, 000372 /№430 /14.04.98 /14.04.2001 /000 «ТопС интегратор систем» /123557, Москва, Пресненский вал, 14, оф. 411, т.253-3632,253-6318 /1.2а-е;2;3а-е;5 /

429 /ЛГ 0008, 000373 /№431 /14.04.98 /14.04.2001 /ЗАО «ИНТЕРКОМСЕРВИС компьютерные сети» /123363, Москва, ул. Новопоселковская, 6, т. 792-3195 /3.1г-е;3.7г-е; 3.2-З.ба-е; 3.8-3.9а-е /

430 /ЛГ0008, 000374 /№432 /14.04.98 /14.04.2001 /000 «ТехИнформКонсалтинг» /121019, Москва, Малый Афанасьевский пер., 5/15,

т. 290-2539,290-2374 /3.3-3.6а-е; 3.8-3.9а-е; 5а (в части защиты от НСД) /

431 /ЛГ0008, 000375 /№433 /14.04.98 /14.04.2001 /Государственный испытательный сертификационный центр программных средств вычислительной техники (Госкомсвязи России) /170023,Тверь, ул. Ржевская, 10, а/я 2337, т. (0822) 44-31-72, 44-40-44 /1.2г-е;3.1г,д /

432 /ЛГ0008, 000376 /№434 /14.04.98 /14.04.2001 /Московский государственный технический университет им. Н. Э. Баумана (Минобразования России) /107005, Москва, 2-я Бауманская ул., 5, т. 263-6955, 263-6522 /1.2;2;3;4;5;6 /

433 /ЛГ0008, 000377 /№435 /21.04.98 /21.04.2001 /ЗАО «Компания «Интертраст» /103001, Москва, Большая Садовая ул., 6, т. 956-7928 /3.1г-е; 3.2-3.9а-е /

434 /ЛГ0008, 000378 /№436 /21.04.98 /21.04.2001 /ООО «Проектно-монтажное предприятие НИЦ «Охрана» /143952, Реутов Московской обл., ул. Молодежная, 1, т. 702-1510 /3.1г-е; 3.2-3.9а-е /

435 /ЛГ0008, 000379 /№437 /21.04.98 /21.04.2001 /Региональный центр по защите информации и проведению специальных экспертиз (Кабинет Министров Республики Татарстан) /420029, Казань, ул. Халитова,3, т. (8432) 76-6283, 76-0484 /1.2а-е;2;3а-е;4; 5а-в /

Продолжение приложения 3

№ п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки

451 /ЛГ0008, 000399 /№453 /17.06.98 /17.06.2001 /ТОО «Научно-производственное внедренческое предприятие «ФОРС» /125267, Москва, Миусская пл., 6, стр. 3, т. 973-4067, 973-4080 /3.1г-е;3.2-3.9а-с /

452 /ЛГ0017, 000801 /№454 /17.06.98 /17.06.2001 /ЗАО «SCAN» /1-17330, Москва, ул. Дружбы, 10/32, корп. Б, т. 232-2343 /3.1г-е;3.2-3.9а-е /

453 /ЛГ0017, 000802 /№455 /19.06.98 /19.06.2001 /ЗАО «Лагрон плюс» /125284, Москва, ул. Беговая, 15, т. 945-5231,945-3507 /3.1-3.4г-е /

454 /ЛГ0017, 000803 /№456 /19.06.98 /19.06.2001 /ООО «Корпорация «ЮНИ» /123022, Москва, 2-я Звенигородская ул., 13, т.956-6444 /3.3-3.6а-е; 3.8-3.9а-е; 5а /

455 /ЛГ0017, 000807 /№457 /19.06.98 /19.06.2001 /Межрегиональное общественное учреждение «Институт инженерной физики» /142210, Московская обл. Серпухов-10, а/я № 351, т. 35-3193 /1.2а-с;2;3а-е;4; 5 /

456 /ЛГ0017, 000808 /№458 /26.06.98 /26.06.2001 /ЗАО «Контур-Сервис ТВ» /357519, Ставропольский край, Пятигорск, ул. Кучуры, 8, т. 4-13-64 /2; 3.3-3.6а-е; 3.8-3.9а-е;4 /

457 /ЛГ0017, 000809 /№459 /26.06.98 /26.06.2001 /ООО «Гарда-S» /414000, Астрахань, ул. Максима Горького, 25, кв.27 /1.2а-е;2;3а-е;4; 5а-в /

458 /ЛГ0017, 000810 /№460 /01.07.98 /01.07.2001 /ЗАО «КОМПАНИЯ ЭР-СТАИЛ» /127273, Москва, ул. Декабристов, 38, к.1, т. 402-7509 /3.1г-е; 3.2-3.9а-с /

459 /ЛГ0017, 000811 /№461 /01.07.98 /01.07.2001 /ООО «УСП КОМПЬЮЛИНК» /117607, Москва, ул. Удальцова, 85, корп. 2, т. 131-4022, 931-9301 /3.1г-е;3.2-3.9а-е 1 /

460 /ЛГ0017, 000813^ /№462 /01.07.98 /01.07.2001 /Центральный научно-исследовательский и опытно-конструкторский институт робототехники и технической кибернетики при СПТУ (Минобразования России) /194064, Санкт-Петербург, Тихорецкий пр.,21, т.(812)552-0110,552-9246 /3г-е /

461 /ЛГ0017, 000813 /№463 /01.07.98 /01.07.2001 /ООО «Информационные

Бизнес Системы» /101511, Москва, ГСП, Дмитровское ш., 9-Б, 967-8010 /3.1г-е 3.3.3.4г. е3.6-3.7г-с 3.9г-е /
462 /ЛГ0017, 000814 /№464 /01.07.98 /01.07.2001 /ГП «ОКБ «КОМПАС-М» /113184, Москва, ул. Землячки, 35, т. 951-3036 /1.2;2;3;4 /
463 /ЛГ0017, 000815 /№465 /01.07.98 /01.07.2001 /АООТ «ИМПУЛЬС» /129626, Москва, пр. Мира, 102, т.287-8873 /3.1-3.26,3.7-3.96 /
464 /ЛГ0017, 000816 /№466 /01.07.98 /01.07.2001 /ОАО «Московская цифровая телефонная компания» /129626, Москва, пр. Мира, 102, т. 287-3459, 217-4942 /3.3-3.9а-б; 56 /
465 /ЛГ0017, 000819 /№467 /07.07.98 /07.07.2001 /ЗАО «НТЦ «Интеллект» /127018, Москва, ул. Образцова, 38, т. 219-0034 /2; 3 /

Продолжение приложения 3

№ п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки

466 /ЛГ0017, 000820 /№468 /10.07.98 /10.07.2001 /ОАО «РИНА РОСТРА» /103064, Москва, ул. Казакова, 16, т. 261-1266 /3.1г-е;3.2-3.9а-е /
467 /ЛГ0017, 000821 /№469 /13.07.98 /13.07.2001 /ЗАО «Фирма ДИАЛОГ-СЕТИ» /109028, Москва, Серебряническая наб., 27А, т. 917-7955 /3г-е /
468 /ЛГ0017, 000822 /№ 470 /17.07.98 /17.07.2001 /ООО «Охранные системы» /454091,Челябинск, ул. Плеханова, 43, т. 38-21-88, 51-20-63 /3.3-3.4а-е; 3.5-3.6а,в /
469 /ЛГ0017, 000823 /№471 /17.07.98 /17.07.2001 /АОЗТ «Инвестиционно-коммерческая фирма ИНКО» /127635, Москва, а/я 28, т. 487-3220 /3.3-3.9а-в /
470 /ЛГ0017, 000824 /№ 472 /17.07.98 /17.07.2001 /ЗАО «Руслан коммуникейшнз» /101830, Москва, Малый Харитоньевский пер., 4, т. 923-1010 /3.1-3.9а-е; 5а-в,д /
471 /ЛГ0017, 000825 /№473 /17.07.98 /17.07.2001 /ЗАО «Научно-произвостенное предприятие «Безопасные Информационные Технологии» /103064, Москва, ул. Казакова, 16, т. 267-2763 /1.2г-е;3г-е /
472 /ЛГ0017, 000826 /№474 /17.07.98 /17.07.2001 /ЗАО «Частное охранное предприятие «Агентство ЛУКОМ-А» /101000, Москва, Сретенский б-р, 11, т.927-4866, 239-1182 /26, г, д, е; 3 .3-3.9а-г /
473 /ЛГ0017, 000828 /№475 /21.07.98 /21.07.2001 /ЗАО «МЕЗОН» /625016, Тюмень, ул. Геологоразведчиков, 6В, т. 23-26-63 /2; 3; 4; 5 /•
474 /ЛГ0017, 000829 /№476 /22.07.98 /22.07.2001 /ЗАО «Центр информационной безопасности» /130091, Новосибирск, Красный пр., 54, т. 21-42-71, 21-72-44 /2.16, г, д,е; 3.3-3.4а-в; 4; 5а-в /
475 /ЛГ0017, 000830 /№ 477 /22.07.98 /22.07.2001 /ОАО «ОКБ «КАРАТ» /644065, Омск, пос. Первомайский, 2, т. 64-54-55 /2.2а; 3.36, г-е; 3.4г-е; 3.9г-е; 5а /
476 /ЛГ0017, 000831 /№478 /22.07.98 /22.07.2001 /Главное управление Центрального банка РФ по Иркутской области /664006, Иркутск, ул. Ленина, 16, т. 24-36-31,33-15-29 /2; 4 /
477 /ЛГ0017, 000833 /№479 /31.07.98 /31.07.2001 /ГУ «Новгородский информационно-аналитический центр» (Администрация Новгородской области) /173005, Новгород, Софийская пл., 1, т.(8162) 131-740 /2.2а,д; 3.3-3.4а,ж;4 /
478 /ЛГ0017, 000834 /№480 /31.07.98 /31.07.2001 /Государственный Сибирский научно-исследовательский институт авиации им. Чаплыгина (Минэкономики России) /630051, Новосибирск, ул. Ползунова, 21, т. 77-01-56 /1.2а,в /
479 /ЛГ0017, 000835 /№481 /31.07.98 /31.07.2001 /ООО «Охранное предприятие С.Б.О. Центр» /249020, Калужская обл., Обнинск, ул.

Курчатова, 41, т. (8439) 49-220,49-231 /2.2; 3а-е; 5а-в /
480 /ЛГ0017, 000836 /№482 /31.07.98 /31.07.2001 /000 «ОЛЬГА» /173003, Новгород, ул. Большая Санкт-Петербургская, 80, Т.(81622)2-68-76 /2; 3.2-3.9а-в /
Продолжение приложения 3
№ п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки
481 /ЛГ0017, 000837 /№483 /31.07.98 /31.07.2001 /000 «Научно-технический центр «Спецтехника» (НТЦ «СПЕЦТЕХНИКА») /103051, Москва, ул. Петровка, 24, т. 928-8167, 928-7313 /2г-е; 3.3-3.9а-в /
482 /ЛГ0017, 000838 /№484 /31.07.98 /31.07.2001 /ЗАО «Бизон 95» /103009, Москва, ул. Тверская, 10, т. 956-6840, 292-1431 /3г-е /
483 /ЛГ0017, 000840 /№485 /03.08.98 /03.08.2001 /АНО «Научно-исследовательский центр cals-технологий «Прикладная логистика» /117926, Москва, 5-й Донской проезд, 21 Б, т. 955-5163 /3.1г-е;3.2-3.9а-е /
484 /ЛГ0017, 000842 /№486 /04.08.98 /04.08.2001 /ОАО «Институт подготовки кадров машиностроения и приборостроения» (Минэкономики России) /141070, Королев Московской обл.. Октябрьский б-р, 80, т.511-5790,511-2065 /б /
485 /ЛГ0017, 000843 /№487 /04.08.98 /04.08.2001 /Кубанский Государственный технологический университет (Минобразования) /350072, Краснодар, ул. Московская, 2, т. 55-84-01, 55-65-67 /6 /
486 /ЛГ0017, 000844 /№488 /05.08.98 /05.08.2001 /ЗАО «ОРЕГОН» /109117, Москва, ул. Окская, 6, корп. 1, т. 974-6006 /3.1г-е;3.2-3.9а-е /
487 /ЛГ0017, 000845 /№489 /05.08.98 /05.08.2001 /000 «Компания Спинакер» /109017, Москва, Пыжевский пер., 7А, корп. 206, т.953-0508,951-6809 /3.1г-е;3.2-3.9а-е /
488 /ЛГ0017, 000847 /№490 /05.08.98 /05.08.2001 /ЗАО «ЭВРИКА» /189640, С.-Петербург, Сестрорецк, наб. р. Сестры,15, т.273-3536 /2; 3.2-3.9а-в; 4; 5а-в /
489 /ЛГ0017, 000848 /№491 /05.08.98 /05.08.2001 /ЗАО «Московская Телекоммуникационная Корпорация» /103051, Москва, ул. Неглинная, 17, стр.2, т. 200-1539, 200-1538 /2; 3.3-3.9; 4; 5а-в /
490 /ЛГ 0004, 000151 /№492 /18.08.98 /18.08.2001 /ОАО «ТЕРНА» /107065, Москва, ул. Уральская, 21, т. 460-0610, 460-0044 /3а-е /
491 /ЛГ 0004, 000152 /№493 /19.08.98 /19.08.2001 /Управление внутренних дел Алтайского края (МВД России) /656025, Барнаул-25, пр. Ленина, 74, т. (385-2) 24-37-47 /2б-е; 3.3 - 3.6а-в; 3.8 -3.9а-в; 4 /
492 /ЛГ0004, 000153 /№494 /27.08.98 /27.08.2001 /000 «ЦИНТУР» /620151, Екатеринбург, ул. Гоголя, 25А, т. (3432) 51-87-82 /2; 3.3-3.9а-е;4 /
493 /ЛГ 0004, 000155 /№495 /27.08.98 /27.08.2001 /000 «МХМ-Защита» /Москва, Большой Патриарший пер., 4, оф. 1-2, т. 291-2754, 203-4413 /2; 3.9а, б, г-е; 3.3-3.6а, б, г-е /
494 /ЛГ 0004, 000157 /№496 /02.09.98 /02.09.2001 /ОАО «Научно-исследовательский институт суперЭВМ» /117437, Москва, ул. Академика Волгина,33, т. 330-2575, 330-0133 /1.2а-е;2;3.1а-е; 3.3-3.9а-е; 4; 5а-в /
495 /ЛГ0004, 000158 /№497 /03.09.98 /03.09.2001 /Управление внутренних дел Калининградской области (МВД России) /236000, Калининград, Советский пр., 7, т. (011-2) 22-6418, 22-6261,21-9867 /2б-е; 3.3-3.6а-в; 3.8-3.9а-в;4 /
Продолжение приложения 3
№ п/п /Серии, номер бланка /Номер лицензии /Дата выдачи /Действительна

до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки
496 /ЛГ 0004, 000159 /№498 /03.09.98 /03.09.2001 /ООО «СКАНЕР» /656099, Барнаул, Комсомольский пр., 73, т. 23-84-46 /2.1д-е;3.5а;3.9а /
497 /ЛГ0004, 000161 /№499 /04.09.98 /04.09.2001 /Управление федерального казначейства по Волгоградской области (Минфин России) /400066, Волгоград, ул. Коммунистическая, 28А, т. 93-61-78, 33-55-04 /6 /
498 /ЛГ 0004, 000163 /№500 /16.09.98 /16.09.2001 /ООО «Комби-Сервис» /357700, Кисловодск Ставропольского края, ул. Клары Цеткин, 39, т. 3-74-82, 3-66-66 /3.2-3.6а-д; 3.8-3.9а-д /
499 /ЛГ0004, 000164 /№501 /16.09.98 /16.09.2001 /Научно-исследовательский институт информационных технологий (Правительство Москвы) /113054, Москва, ул. Бахрушина, 18, стр.3, т. 235-4924 /3.1г-е; 3.2-3.9а-е /
500 /ЛГ0004, 000168 /№502 /22.09.98 /22.09.2001 /ООО «ЭНСАНОС» /103051, Москва, ул. Петровка, 24, стр. 3, т. 928-8167 /3а, б /
501 /ЛГ 0004, 000169 /№503 /23.09.98 /23.09.2001 /ООО «Научно-производственная лаборатория «ИНФО-КРИПТ 2000» /113405, Москва, Варшавское ш., 125,т.330-5156 /1.2;2;3;4;5а-в /
502 /ЛГ 0004, 000170 /№504 /29.09.98 /29.09.2001 /ЗАО «Инжиниринг + Электроникс» /113405, Москва, Варшавское ш., 125, т. 975-3273 /2; 3а-е; 4;5 /
503 /ЛГ 0004, 000171 /№505 /29.09.98 /29.09.2001 /ООО «Научно-технический центр «ЮНИСЕРВ» /113587, Москва, а/я 107, т.319-4956,319-1156,319-7945 /2; 3а-е;4 /
504 /ЛГ 0004, 000172 /№506 /30.09.98 /30.09.2001 /ЗАО «ЛАНИТ-СИСТЕМ» /107066, Москва, ул. Доброслободская, 5, стр.1, т. 267-8750 /1.2;2;3;5а-в;6 /
505 /ЛГ 0004, 000173 /№507 /08.10.98 /08.10.2001 /ООО «НАВИГАТОР» /626718, Новый Уренгой Тюменская обл., ул. 26-го съезда КПСС, 2, корп. 105, т. (31519) 4-8025 /3.1г-е; 3.2-3.9а-е /
506 /ЛГ 0004, 000174 /№508 /12.10.98 /12.10.2001 /ТОО «Научно-внедренческое предприятие «Информация Экономика» (НВП «ИНЭК») /125171, Москва, Ленинградское ш., 16,т.150-8608,150-9213 /3.1г-е; 3.2-3.9а-е /
507 /ЛГ 0004, 000175 /№509 /13.10.98 /13.10.2001 /ЗАО «Микротест» /620142, Екатеринбург, ул. Щорса, 15, т. (3432) 222-155 /1.2r-е; 3.1г-е; 3.2-3.9а-е /
508 /ЛГ 0004, 000176 /№510 /14.10.98 /14.10.2001 /ООО Фирма «ДАТА-ЦЕНТР» /б20098,Екатеринбург, а/я 176, т. (3432) 45-83-49,46-77-31 /3;4;5а,б /
509 /ЛГ 0004, 000177 /№511 /14.10.98 /14.10.2001 /ЗАО «Корус АКС» /620034, Екатеринбург, ул.Егора Сазонова, 70, комн.2 т. (3432) 56-82-96,56-22-88, т./факс 55-55-29 /3;5а,б /

Продолжение приложения 3

Кг п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки
510 /ЛГ 0004, 000180 /№512 /22.10.98 /22.10.2001 /ЗАО «Спецмонтажстрой-5» (СМС-5) /127566, Москва, ул. Бестужевых, 25В, т. 902-0 111 /2; 3а-е; 4; 5 /
511 /ЛГ 0004, 000181 /№513 /22.10.98 /22.10.2001 /ООО «Безопасность бизнеса» /197061, Санкт-Петербург, ул. Большая Монетная, 17, т. 252-7762, т./факс 252-7762 /2.1е;3а-в /

512 /ЛГ 0004, 000182 /№514 /22.10.98 /22.10.2001 /ЗАО «РОССИ СЕКЬЮРИТИ» /119435, Москва, Саввинская наб., 25,т.245-8907,245-8063 /3.2-3.6а-е; 3.8-3.9а-е /

513 /ЛГ 0004, 000183 /№515 /29.10.98 /29.10.2001 /Краснодарский филиал Государственного унитарного предприятия Научно-технический центр «Атлас» (ФАПСИ) у /350068, Краснодар, ул. Красноармейская, 20, т. (8612) 644-593,686-767, т./факс (8612) 680-242 /2а, б, г, д. е; 3.3-3.6а-е; 3.8-3.9а-е; 4 /

514 /ЛГ 0004, 000184 /№516 /04.11.98 /04.11.2001 /ЗАО «РЕСУРСИНФОРМ» /117335, Москва, а/я 4, т. 769-0736 /3.1г-е;3.2-3.9а-е /

515 /ЛГ 0004, 000185 /№517 /04.11.98 /04.11.2001 /000 «ТОРА» /660021, Красноярск, ул. Красной Армии, 28, т. (391-2) 217-588 /3.1г-е;3.2-3.9а-е /

516 /ЛГ0004, 000186 /№518 /04.11.98 /04.11.2001 /000 «ГЕО СПЕКТРУМ» /109316, Москва, Волгоградский пр., 45,т.177-8182, 917-5115 /3а-е /

517 /ЛГ 0004, 000188 /№519 /10.11.98 /10.11.2001 /ЗАО «ИНФОКРИСТАЛ» /129090, Москва, ул. Гиляровского, 2/5, т. 207-7469 /3.1г-е;3.2-3.9а-е /

518 /ЛГ0004, 000190 /№520 /18.11.98 /18.11.2001 /000 «Охранное агентство «Стрелец-М» /119435, Москва, Большой Саввинский пер., 14/2, т. 248-4106 /3.3-3.9а-е /

519 /ЛГ0004, 000191 /№521 /23.11.98 /23.11.2001 /000 «Научно-производственное объединение «КРИПТЕН» /141980, Дубна Московской обл., ул. Приборостроителей, 2, комн. 308, т. (09621) 220-18 /3.1г-е;3.2-3.9а-е /

520 /ЛГ0004, 000192 /№522 /24.11.98 /24.11.2001 /ЗАО «Алкорсофт» /198900, Санкт-Петербург, ул. Радищева, 39, Т.(812)329-1780 /3.1-3.4 г-д; 3.9г,д /

521 /ЛГ 0004, 000193 /№523 /24.11.98 /24.11.2001 /Государственное учреждение «Калининградский государственный научно-исследовательский центр информационной и технической безопасности» (Администрация Калининградской области) /236007, Калининград, ул. Дмитрия Донского, 1, т. (0112) 46-75-50,22-58-01 /1.2а-в;2;3.2а.в; 3.Э-3.9а-е;4;5а-в /

522 /ЛГ0004, 000194 /№524 /24.11.98 /24.11.2001 /000 «Конфидент» /193148, Санкт-Петербург, пр. Большой Смоленский, 36, т. (812)325-1037,568-1035 /2; 3:4; 5*4 /

Продолжение приложения 3

№ п/п /Серия, номер бланка /Номер лицензии /Дат» выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки

523 /ЛГ 0004, 000195 /№525 /25.11.98 /25.11.2001 /Краевое государственное предприятие унитарное предприятие «Приморпродукт-контроль» /690091, Владивосток, ул. Светланская, 115,каб.47, т. (4232) 26-40-75,26-03-57 /3.1г-е; 3.2-3.9а-е /

524 /ЛГ 0004, 000196 /№526 /27.11.98 /27.11.2001 /ЗАО «ГОЛЛАРД» /103001, Москва, Б.Садовая ул., 1, стр.1, т. 251-0164 /3.1г-е;3.2-3.6а-е; 3.8-3.9а-е /

525 /ЛГ 0004, 000197 /№527 /04.12.98 /04.12.2001 /Управление внутренних дел Новосибирской области (МВД) /630099, Новосибирск, ул. Октябрьская, 78, т. (383-2) 16-71-00, 16-70-33 /2б-е; 3.3-3.6а-в; 3.8-3.9а-в;4 /

526 /ЛГ 0004, 000198 /№528 /07.12.98 /07.12.2001 /ЗАО «СИГНАЛ-КОМ» /115230, Москва, а/я 1, т.111-6358,11-63-67 /1.2г-е;2.2а,б; 3а, в-е /

527 /ЛГ 0004, 000200 /№529 /10.12.98 /10.12.2001 /Дочернее открытое акционерное общество «Оргэнергогаз» /142717, Московская обл., Ленинский

р-н, п/о Развилка, т. 355-9321 - /2;3;4;5 /
528 /ЛГ 0003, .000102 /№530 /11.12.98 /11.12.2001 /ОАО Концерн «Российские защитные технологии» /101485, Москва, ГСП-4, ул. Селезневская, НА, стр. 2, т.491-9112,491-8789 /3.1г-е;3.2-3.9а-е /
529 /ЛГ 0003, 000103 /№531 /16.12.98 /16.12.2001 /000 «Центр технических средств защиты информации» /620102, Екатеринбург, ул. Начдива Васильева,1,т.23-24-15 /2; 3.2-3.9а-е; 4; 5а-в /
530 /ЛГ 0003, 000105 /№532 /22.12.98 /22.12.2001 /000«СИБЗНАК» /660021, Красноярск, ул. Копылова, 2А, т. 65-24-15,21-63-98 /3.1г-е; 3.2-3.9а-е /
531 /ЛГ0003, 000106 /№533 /22.12.98 /22.12.2001 /000 «Охранное предприятие «АРГУС» /113149, Москва, ул. Сивашская, 4,стр.2,т.318-9611 /2;3а-е /
532 /ЛГ 0003, 000109 /№534 /25.12.98 /25.12.2001 /ТОО Производственно-техническое предприятие «БИТКОМ» /123308, Москва, пр. Маршала Жукова, 9, а/я 8, т. 197-0347 /3г-с /
533 /ЛГ0003, 000111 /№535 /29.12.98 /29.12.2001 /ТОО Частное охранное предприятие «Алмаз» /141070, Королев Московской обл., ул. Дзержинского, 9, т. 513-4873 /3.1а,г,д;3.2г,д; 3.3-3.9а,г,д /
534 /ЛГ 0003, 000112 /№536 /29.12.98 /29.12.2001 /000 «Научно-производственная фирма «ГЕЙЗЕР» /117909, ГСП-1, Москва, В-49, 2-й Спасоналивковский пер., 6, т. 230-0374 /2; 3.3-3.4а-е; 3.5а-в; 3.6а-е; 3.7-3.8а-в; 3.9а-е; 4; 5а-в /
535 /ЛГ 0003, 000113 /№537 /13.01.99 /13.01.2002 /000 частное охранное предприятие «Межрегиональная информационно-техническая фирма» /Тольятти Самарской обл., ул. Баныкина,50,кв. 286, т. 39-09-02 /2; 3а-е;4 /

Продолжение приложения 3

№ п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки
536 /ЛГ ООО3, 000114 /№538 /19.01.99 /19.01.2002 /Технический Центр федеральной службы налоговой полиции России (ФСНП России) /101968, Москва, ул. Маросейка, 12, т. 917-7982,917-7499 /2; 4 /
537 /ЛГ 0003, 000116 /№539 /22.01.99 /22.01.2002 /Дочернее ОАО «Гипрогазцентр» РАО «Газпром» /603600, Нижний Новгород, ул. Алексеевская, 26, Т.(8312)35-08-38 /2; 3а-д; 4; 5 /V
538 /ЛГ 0003, 000118 /№540 /29.01.99 /29.01.2002 /Государственное унитарное предприятие НТЦ «Юграспецтехнологии» (Администрация Ханты-Мансийского автономного округа) /626200, Ханты-Мансийск Тюменской обл., Ханты-Мансийский автономный округ, ул. Мира, 110А, т. 3-39-31,3-46-71 /2г-е; 3.3-3.9а-е; 5а-в /
539 /ЛГ 0003, 000119 /№541 /02.02.99 /02.02.2002 /000 «Нижегородская Межотраслевая Лаборатория» /603000, Нижний Новгород, Гребешковский откос, 7, оф. 10, Т.(8312)30-34-12 /3.3-З.ба-в /
540 /ЛГ 0003, 000121 /№542 /02.02.99 /02.02.2002 /ЗАО «Региональные информационно-телекоммуникационные системы «РИНТЕКС» /302028, Орел, ул. Октябрьская, 42А, т. (08622) 5-38-14 /2; 3а-е; 4; 5а, б /
541 /ЛГ 0003, 000122 /№543 /05.02.99 /05.02.2002 /Государственный научно-исследовательский институт моделирования и интеллектуализации сложных систем /197376, Санкт-Петербург, ул. Профессора Попова, 5, т. (812)234-0415,234-9094 /3г-е /
542 /ЛГ 0003, 000123 /№544 /05 02.99 /05 02.2002 /ЗАО Частное охранное предприятие «ЛЕГИОН—Х» /103009, Москва, ул. Тверская, 14, стр. А, т. 229-4419, 200-0033 /3а-е /

543 /ЛГ 0003, 000124 /№545 /15 02.99 /15.02.2002 /Государственное ордена «Знак Почета» предприятие электрорадионавигации и спутниковой связи— МОРСВЯЗЬСПУТНИК (Министерство транспорта РФ) /115230, Москва, Варшавское ш., 42,т.967-1862, 967-1850 /1.2г-е;2;3а-с; 5а-в - /
544 /ЛГ 0003, 000125 /№546 /18.02.99 /18.02.2002 /ОАО «Московский завод счетно-аналитических машин им. В. Д. Калмыкова» /107066, Москва, ул. Нижняя Красносельская, 35,т.261-1204 /2; 3а-е; 4 /
545 /ЛГОООЗ, 000126 /№547 /18.02.99 /18.02.2002 /ЗАО «ПОЛЕТ—ЭЛИТА» /109147,Москва, ул. Марксистская, д.34,стр.5,т.912-1312 /3.2-3(9а,в /
546 /ЛГ 0003, 000127 /№548 /18.02.99 /18.02.2002 /ООО «Агентство «Шериф» /173003, Великий Новгород, ул. Большая Санкт-Петербургская, 64, т. (8162) 22-46-94 /2.1а,д /
547 /ЛГОООЗ, 000136 /№549 /18.02.99 /18.02.2002 /ООО «Частное охранное предприятие «Гарант» /125124, Москва, Саввинская наб., 5,т.248-3115 /2г-е; 3.4-3.9а-е /
548 /ЛГОООЗ, 000131 /№550 /19.02.99 /19.02.2002 /ЗАО «Открытые технологии-98» /117036, Москва, ул. Дм. Ульянова, д.7а,т. 132-7005 /1.2г-е;2.2а,б; 3.1-3.2г-е; 3.3-3.9; 5а, б/

Продолжение приложения 3

№ п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки

549 /ЛГ 0003, 000132 /№551 /19.02.99 /19.02.2002 /ЗАО «АГРОФИНТРЕИД» /103009. Москва, Б. Гнездниковский пер., 3/5, стр. 2, т. 229-0018 (44-42) /3.3а /
550 /ЛГ0003, 000133 /№552 /19.02.99 /19.02.2002 /ООО «Европеум-групп» /121019, Москва, Б. Знаменский пер., 4, т. 203-4435 /3.1г-е;3.2-3.6а-е; 3.7г-е; 3.8-3.9а-е/
551 /ЛГ0003, 000135 /№553 /25.02.99 /25.02.2002 /ЗАО «Компания «Кардинал» /630004, Новосибирск, ул. Челюскинцев, 18, т. (383-2)101-917,101-275 /2.1а,б,г-е; 3.3а-г; 3.4а, в, г; 3.5а, в; 3.6а, в, г; 3.9а-в; 4; 5а, б /
552 /ЛГ 0003, 000137 /№554 /26.02.99 /26.02.2002 /ЗАО «Корпорация коммуникационных систем (ККС)» /107066, Москва, ул. Старая Басманная, 26, т. 265-4192 /3.1г-е;3.2-3.9а-е /
553 /ЛГ 0003, 000138 /№555 /26.02.99 /26.02.2002 /ООО «Защита информации» /620075, Екатеринбург, ул. Мичурина, 47-22, т. 56-04-38 /3.1г-е;3.2-3.6а-е; 3.7г-е; 3.8-3.9а-е /
554 /ЛГ0003, 000139 /№556 /10.03.99 /10.03.2002 /Государственный специализированный проектный институт (Минатом России) /107014, Москва, ул. Новорязанская, 8а, т.925-0813,261-1259 /5 /
555 /ЛГ 0003, 000140 /№557 /10.03.99 /10.03.2002 /Негосударственное образовательное учреждение повышения квалификации «Научно-информационный центр проблем безопасности» /193148, Санкт-Петербург, а/я 62, т. (812) 265-1911,325-1037, 568-1035 /6 /
556 /ЛГ0003, 000141 /№558 /10.03.99 /10.03.2002 /ООО Научно-производственное предприятие «КВАЗАР-Ц» /141070, Королев Московской обл., ул. Пионерская, 4, Т.(095)913-5100 /1.2а-е;2а-е; 3а-е; 4; 5а-в /
557 /ЛГ0003, 000142 /№559 /11.03.99 /11.03.2002 /ОАО «Кирово-Чепецкий комбинат им. Б. П. Константинова» /613-020, Кирово-Чепецк Кировской обл., пер. Пожарный, 7Л. (8332), 62-48-29 доб.42-51, доб. 49-33 /2; 3.3-3.9а-е; 4; 5а, д, с /
558 /ЛГ0003, 000143 /№560 /11.03.99 /11.03.2002 /ЗАО «ИНТЕЛЛЕКТ-СЕРВИС» /109172, Москва, ул. Гончарная, 27,т.915-6180 /3г-е /

559 /ЛГ0003, 000147 /№561 /18.03.99 /18.03.2002 /ЗАО «ХОЛМРОК» /236039, Калининград, ул. Октябрьская, 71/73, т. (0112) 44-16-44 /3.3б /
560 /ЛГ0003, 000148 /№562 /19.03.99 /19.03.2002 /000 Научно-промышленная компания «Секьюрити центр С & Т» /107120, Москва, ул. Н. Сыромя-тинская,10,т.916-7976 /3.2-3.6а-е; 3.8-3.9а-е /
561 /ЛГ0003, 000149 /№563 /24.03.99 /24.03.2002 /ЗАО «АО Кворум» /113114, Москва, Шлюзовая наб., 6, т.232-1731,235-7396 /1.2г-е;3г-е /
Продолжение приложения 3
№ п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки
562 /ЛГ0003, 000150 /№564 /24.03.99 /24.03.2002 /ЗАО «ГРАФИКЭЛ СЕКЬЮРИТИ» /121019, Москва, ул. Новый Арбат, 19, оф. 515, т. 291-8161 /3.3а /
563 /ЛГ 0002, 000053 /№565 /26.03.99 /26.03.2002 /000 «Гранит» /600001, Владимир, ул. Московская, 27а /2; 3а-е;4 /
564 /ЛГ0002, 000054 /№566 /26.03.99 /26.03.2002 /ЗАО специализированное конструкторское бюро «ТЭЛКА» /123100, Москва, Шмитовский пр., 2, стр. 2, т. 261-4191 /3.2-3.66, г-е; 3.8-3.96, г-е; 5а-в /
565 /ЛГ0002, 000055 /№567 /6.04.99 /6.04.2002 /Государственное «Дальневосточное региональное предприятие АВТОМАТИКА и СВЯЗЬ» /680000, Хабаровск, ул. Гоголя, 14, т. (4212) 39-34-59 /3.3а, б; 3.5а, б; 3.6а, б /
566 /ЛГ 0002, 000056 /№568 /6.04.99 /6.04.2002 /ОАО «Промэлектромонтаж» /107370, Москва, ул. Бойцовая, 27,т. 60-27-10 /3а-е; 5а /
567 /ЛГ 0002, 000057 /№569 /6.04,99 /6.04.2002 /ЗАО «Научно-производственная фирма ЭЛИНВЕСТ» /103575, Москва, Зеленоград, корп.100, т. 444-2558, 729-2241 /1.2г-е;2.2а; 3.1-3.2г-е; 3.3-3.9а-е; 5а /
568 /ЛГ 0002, 000059 /№570 /9.04.99 /9.04.2002 /000 «КРАЙС ИНФОРМ» /660021, Красноярск, ул. Красной Армии, 28, т. (391-2) 211-478 /3а-е /
569 /ЛГ0002, 000064 /№572 /19.04.99 /19.04.2002 /СП ЗАО «Центр артеграфики «РОССИТА» /300600, Тула, Красноармейский пр., 48, т. (0872) 30-55-03 /3а-в /
570 /ЛГ0002, 000065 /№573 /19.04.99 /19.04.2002 /ОАО «ВЫМПЕЛ-КОММУНИКАЦИИ» /125083, Москва, ул. 8 Марта, 10/12, т. 212-0512 /2; 3а-е /
571 /ЛГ0002 000068 /№574 /22.04.99 /22.04.2002 /ОАО «Калужский турбинный завод» /248632, Калуга, ул. Московская, 225, т. (084-22) 56-30-56 /2; 33-3.8а, б, г-е; 4 /
572 /ЛГ 0002, 000069 /№575 /27.04.99 /27.04.2002 /000 «Славсервисвязь» /302020, Орел, Наугорское ш., 5, т. (0862) 43-22-08 /1.2а-е;2;3а-е;4 /
573 /ЛГ0002 000070 /№576 /27.04.99 /27.04.2002 /000«МАЛТИТЕК» /101509, Москва, ул. Лесная, 43, стр.1, т. (095) 973-5391 /3а-е /
574 /ЛГ0002 000071 /№577 /27.04,99 /27.04.2002 /000 «Контур-М» /630091, Новосибирск, ул. Фрунзе, 5, т. (383-2) 66-51-25 /3.3а, в, г /
575 /ЛГ0002, 000072 /№578 /29.04.99 /29.04.2002 /000 «Рубеж-92» /Москва, Б. Девятинский пер., 4, т. (095) 255-9000 /2; 3а-е; 4; 5 /
576 /ЛГ0002, 000073 /№579 /30.04.99 /30.04.2002 /АОЗТ «СТИНС КОМАН» /105203, Москва, ул. Первомайская, 126, т. (095) 465-4763 /2.2; 3а-е; 5а-в /
577 /ЛГ0002 000074 /№580 /05.05.99 /05.05.2002 /ГП «Центр информационных технологий и систем органов исполнительной власти — ЦИТиС» (ФАПСИ) /123557, Москва, Пресненский вал, 17, т. (095) 737-0110 /2; 3а-е; 5а-в /
Продолжение приложения 3

№ п/п /Серия, номер /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки
578 /ЛГ0002, 000075 /№581 /12.05.99 /12.05.2002 /000 Частное охранное предприятие «Альфа-МоТС» /107078, Москва, ул. Новая Басманная, 18,стр,1,т. (095) 267-5101 /3.3-3.9а-е /
579 /ЛГ0002 000077 /№582 /13.05.99 /13.05.2002 /ЗАО «И.К.ИНТЕРПРАКС» /Москва, ул. Архитектора Власова, 55, оф. 406, т. (095) 128-4884 /3а-е /
580 /ЛГ0002 000078 /№583 /13.05.99 /13.05.2002 /Министерство внутренних дел Республики Карелия (МВД России) /185630, Петрозаводск, пр. Карла Маркса, 18, т. (814-2) 77-4085 /2б-е; 3.3-3.6а-в; 3.8-3.9а-в;4 /
581 /ЛГ0002, 000079 /№584 /21.05.99 /21.05.2002 /Государственное унитарное предприятие «Конструкторское бюро «Связьморпроект» (Минэкономики России) /190000, С.-Петербург, ул. Малая Морская, 14, т. (812) 312-8268 /3а; 4 /
582 /ЛГ0002, 000080 /№585 /25.05.99 /25.05.2002 /000 «ЭЛКО Технологии СПБ» /193036, С.-Петербург, ул. Гончарная, 36, т. (812) 277-7175, 327-3936 /3а,б,г,д /
583 /ЛГ0002, 000082 /№586 /25.05.99 /25.05.2002 /ЗАО Акционерный коммерческий банк «ЗАЛОГБАНК» /119435, Москва, ул. Погодинская, 24, стр. 1, т. (095) 737-0000 /3а-е /
584 /ЛГ0005, 000221 /№587 /20.07.99 /20.07.2002 /ЗАО «ЛАМПОРТ Системз» /117218, Москва, ул. Кедрова, 14, стр.1, т. 719-0609, 719-0709 /2.1а-г;3 /
585 /ЛГ0002, 000084 /№588 /28.05.99 /28.05.2002 /Рязанская государственная радиотехническая академия (Минобразования России) /391000, Рязань, ГСП, ул. Гагарина, 59/1, т. (0912) 72-18-44,72-18-30 /2; 3а-е; 4; 5а-в; 6 /
586 /ЛГ0002, 000086 /№589 /05.06.99 /05.06.2002 /000 «Криптон» /167000, Сыктывкар, ул. Пермская, 14А, т. (8212)44-22-97 /2а, г-е; 3.3-3.9а-е /
587 /ЛГ0002, 000087 /№590 /07.06.99 /07.06.2002 /000 «Телекоммуникационная компания» «ГУТА» /101959, Москва, ул. Мясницкая, 35, т. (095) 204-1712, 204-1715 /2; 3.2 – 3.6а-д; 3.8 – 3.9а-д; 5 /
588 /ЛГ0002, 000088 /№591 /08.06.99 /08.06.2002 /Государственное испытательно-контрактное предприятие «РИТМ» (Минэкономики России) /115487, Москва, ул. Садовники, 4, т. (095) 118-8592,118-8644 /2;3;4 /
589 /ЛГ0002, 000090 /№592 /10.06.99 /10.06.2002 /Дочернее государственное унитарное научно-исследовательское предприятие «АРГУС» (Минэкономики России) /440061, Пенза, ул. Советская, 9, т. (095)118-8592,118-8644 /3а-е; 5а-в /
590 /ЛГ0002, 000091 /№593 /17.06.99 /17.06.2002 /Войсковая часть 20559-А (Минобороны России) /103175, Москва, Б. Козловский пер., 6, т. (095) 204-2402,204-2587 /1.2а-в;2;3.7а-в; 3.9а-в; 4 /
591 /ЛГ0002, 000093 /№594 /21.06.99 /21.06.2002 /АОЗТ «Всесоюзный институт волоконно-оптических систем связи и обработки информации» /107066, Москва, ул. Н. Красносельская, 13, корп. 1, т. 267-2031,267-3089/1.2а-е;2;3;4; 5а-в /

Продолжение приложения 3

№ п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки
592 /ЛГ 0002, 000094 /№595 /21.06.99 /21.06.2002 /Концерн «Системпром» /107066, Москва, ул. Н. Красносельская, 13,корп.1, т. 267-2031,267-3089 /1.2а-е;2;3;4;5 /

593 /ЛГ 0002, 000095 /№596 /23.06.99 /23.06.2002 /Производственный кооператив «Бюро информационной технологии» /103062, Москва, Подсосенский пер.,26,стр.2,т.916-1780 /3.16, д; 3.4-3.66, д; 3.96, д /
594 /ЛГ 0002, 000096 /№597 /23.06.99 /23.06.2002 /ОАО «КРАСНОЯРСКЭНЕРГО» /660021, Красноярск, ул. Борада, 144А., т. 21-96-32.21-04-43 /2.1 /
595 /ЛГ 0002, 000097 /№598 /28.06.99 /28.06.2002 /ЗАО Охранное предприятие «Центр экономической безопасности» /142770, Московская обл., Ленинский р-н, пос. Газопровод, п/о Коммунарка, т. 428-7406 /3а-е /
596 /ЛГ 0002, 000098 /№599 /28.06.99 /28.06.2002 /Тульский государственный университет (Минобразования России) /300600, Тула, пр. Ленина, д. 92, т. (0872) 33-24-45, 35-34-44 /б /
597 /ЛГ 0005, 000210 /№600 /06.07.99 /06.07.2002 /ООО «АйСиэС Новые системы» /107082, Москва, ул. Ф.Энгельса, д. 67,т.755-6819 /2а-е; 3а-е; 5 /
598 /ЛГ 0005, 000206 /№601 /01.07.99 /01.07.2002 /ООО «НАВСИ» /193130, С.-Петербург, ул. 8-я Советская, 8, т. (812)586-2166 /3.2 - 3.3б; 3.5б; 3.9 /
599 /ЛГ 0005, 000207 /№602 /01.07,99 /01.07.2002 /ГУП «Производственное объединение «Баррикады» (Минэкономики России) /400071, Волгоград, пр. Ленина, т. (8442) 78-19-00 /2.1а,в-е; 2.2а, г-е; 3.3а-в; 3.4а-е;3.5а-в; 3.9а /
600 /ЛГ0005, 000208 /№603 /01.07.99 /01.07.2002 /ГП Особое конструкторское бюро «Спектр» при Рязанской государственной радиотехнической академии (Минобразования России) /390005, Рязань, ГСП, ул. Гагарина, 59/1, т. (0912) 72-18-59, 72-18-44 /3а-е; 5а-в /
601 /ЛГ 0005, 000209 /№604 /01.07.99 /01.07.2002 /ООО Частное охранное предприятие «Команда-АС» /113447, Москва, Севастопольский пр., 15, стр.1,т.415-1095 /2а, г-е; 3.3-3.9а-е /
602 /ЛГ0005, 000211 /№605 /06.07.99 /06.07.2002 /Главное Управление внутренних дел администрации Самарской области (МВД России) /443099, Самара, ул. Куйбышева, 42, т. (846-2) 39-55-43,70-42-14 /2б-е; 3.3-3.9а-в; 4 /
603 /ЛГ 0005, 000213 /№606 /12.07.99 /12.07.2002 /ГУП «Специальное научно-производственное объединение «Элерон» (Минатом России) /115563, Москва, ул. Генерала Белова, 14,т.399-9964, 393-9072 /3а-е;5 /
604 /ЛГ 0005, 000217 /№607 /15.07.99 /15.07.2002 /Автономная некоммерческая организация Учебный центр «ИНФОРМЗАЩИТА»/127018, Москва, а/я 55, т.289-4232,289-8998 /6 /
605 /ЛГ0005, 000218 /№608 /15.07.99 /15.07.2002 /Московский государственный технический университет гражданской авиации (Минобразования) /125837, ГСП-47, Москва, Кронштадтский б-р, 20, т. 459-0707 /2; 3а-е; 4; 5а-в; 6 /

Продолжение приложения 3

№ п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки

606 /ЛГ0005, 000219 /№609 /15.07.99 /15.07.2002 /Самарский государственный технический университет (Минобразования) /443010, Самара, ул. Галактионовская, 141, т. (8-462) 32-16-92, 37-15-77 /2; 3а-е; 4; 6 /
607 /ЛГ0005, 000222 /№610 /20.07.99 /20.07.2002 /ЗАО «Промстройпроект» /119827, ГСП, Москва, Г-48, Комсомольский пр., 42, т. 245-9675 /5 /
608 /ЛГ 0005, 000225 /№611 /21.07.99 /21.07.2002 /ООО «Производственно-

коммерческая фирма «ФЕТАР» /660078, Красноярск, ул. Сурикова, 12, т. (3912) 61-55-30 /3а-е /
609 /ЛГ 0005, 000227 /№612 /22.07.99 /02207.2002 /000 «Частное охранное предприятие «Авторитет» /121351, Москва, ул. Академика Павлова, 12, стр.3, т. 141-6565,415-7155 /2а, г-е; 3.3-3.9а-е /
610 /ЛГ 0005, 000231 /№613 /03.08.99 /03.08.2002 /ОАО «Центральный телеграф» /103375, Москва, ул. Тверская, 7, т.230-2194,924®004 /2а-е /
611 /ЛГ0005, 000233 /№614 /04.08.99 /04.08.2002 /ЗАО Региональный аттестационный центр «ГОСТА» /426057, Ижевск, ул. Горького, 90, Т.(3412)25-0466 /2;3.1-3.2а,в-е; 3.3-3.9а-е; 4; 5а-в /
612 /ЛГ0005, 000234 /№615 /04.08.99 /04.08.2002 /000 «фактор—ТС» /123557, Москва, а/я 8, т.253-5620 /3.1г-е;3.2-3.6а-е; 3.7г-е; 3.8-3.9а-е /
613 /ЛГ0005, 000235 /№616 /06.08.99 /06.08.2002 /000 «Научно-производственное предприятие «АЛЬТАНТ» /111024, Москва, ул. Авиамоторная / /
614 /ЛГ 0005, 000238 /№617 /11.08.99 /11.08.2002 /ЗАО «Ланк» /191186, Санкт-Петербург, наб. р. Мойки, т. (812) 325-6666 /3.3-3.6б, г, д; 3.8-3.9б, г, д 3.5а, в; 3.6г; 3.9а, /
615 /ЛГ 0005, 000239 /№618 /11.08.99 /11.08.2002 /000 Производственно-коммерческая фирма «ФАН и ГП» /650099, Кемерово, пр. Советский, 60, оф. 350, т. (384-2) 36-63-06 /2.1а,б,е; 2.2а-в, д, е; 3.3а, в-е; 3.4в-е; 4; 5а, б,е /
616 /ЛГ 0005, 000241 /№619 /13.08.99 /13.08.2002 /000 «МИКРОТЕСТ—ТЕЛ» /113035. Москва, ул. Содовническая, д.76, корп. 3, т.951-3366,961-2439 /1.2а-е; 2; 3а-е; 4; 5а-в /
617 /ЛГ0005, 000242 /№620 /16.08.99 /16.08.2002 /Управление внутренних дел Омской области (МВД России) /644099, Омск, ул. Ленина, 2,т.(381-2) 29-32-37, 29-36-66 /2б-с; 3.3-3.9а-в; 4 /
618 /ЛГ0005, 000243 /№621 /19.08.99 /19.08.2002 /ОАО "ЛОМО" /194044, Санкт-Петербург, ул. Чугунная, 20, т. (812) 248-5047,248-5242 /2;3а-в;4 /

Окончание приложения 3

№ п/п /Серия, номер бланка /Номер лицензии /Дата выдачи /Действительна до /Наименование предприятия (ведомственная принадлежность) /Адрес предприятия (организации), телефон /Виды деятельности /Особые отметки

619 /ЛГ0005, 000244 /№622 /19.08.99 /19.08.2002 /Институт Проблем управления им. В. А.Трапезникова Российской Академии наук (РАН) /117806, ГСП-7, Москва, ул. Профсоюзная, 65, т.334-7590,334-8910 /3а-е; 5а-в /
620 /ЛГ 0005, 000245 /№623 /20.08.99 /20.08.2002 /Главное Управление внутренних дел Санкт-Петербурга и Ленинградской области (МВД России) /191194, Санкт-Петербург, Литейный пр., 4, т.(812)278-2295,278-3541 /2б-е; 3.3-3.9а-в; 4 /
621 /ЛГ0005, 000249 /№624 /31.08.99 /31.08.2002 /000 «Фирма «Финансовые Операционные Компьютерные Системы» /129085, Москва, пр. Мира, 81, стр.1, т. 287-0811 /3а-е /
622 /ЛГ0006, 000251 /№625 /01.09.99 /01.09.2002 /000 НАУЧНО-ПРОИЗВОДСТВЕННАЯ ФИРМА «РОМБ+К4» /129626, Москва, а/я 36, т. 287-9611,284-1516 /2.1;3.3-3.6а-е; 3.8-3.9а-е /
623 /ЛГ0006, 000252 /№626 /01.09.99 /01.09.2002 /000 «Частное охранное предприятие РиК плюс» /103051, Москва, ул. Садовая-Сухаревская,16,стр.1, т.208-6044 /3а-е /
624 /ЛГ 0006, 000254 /№627 /01.09.99 /01.09.2002 /000 «СЕПТИМА Лтд.»

/101000, Москва, ул. Мясницкая, 17, стр. 1, т. 923-0723 /1.2; 2; 3; 4; 5а-в /
625 /ЛГ 0006, 000255 /№628 /01.09.99 /01.09.2002 /Международный центр услуг гражданской авиации 000 «ВЕРТИКАЛЬ-АВИА» /Москва, Волоколамское ш., 32, корп.1, оф. 44, т. 490-6070 /1.2г-е;3г-ж /
626 /ЛГ0006, 000256 /№629 /07.09.99 /07.09.2002 /Приборостроительный завод (Минатом России) /456080,Трехгорный Челябинской обл., ул. Заречная, 13, т. (351-11) 5-51-36,5-51-21 /2;3;4;5 /
627 /ЛГ0006, 000257 /№630 /08.09.99 /08.09.2002 /000 «ФОБОС ПЛЮС» /117218, Москва, ул. Кржижановского, 21/33, т. 124-0810 /3а-е;5 /
628 /ЛГ0006, 000258 /№631 /08.09.99 /08.09.2002 /АОЗТ «НОВЫЙ АТЛАНТ» /125252, Москва, а/я 51, т.158-0216, 158-0289 /3а-е /
629 /ЛГ 0006, 000259 /№632 /08.09.99 /08.09.2002 /Федеральное ГУП «Центральный НИИ «Комета» (Минэкономики России) /109280, Москва, ул. Велозаводская, 5,т.275-3374,275-0701 /1.2а-е;2;3а-е;4 /
630 /ЛГ 0006, 000261 /№633 /09.09.99 /09.09.2002 /000 «Радиокоммуникационные системы» /191186, С.-Петербург, наб. р. Мойки, 20, т. (812) 325-8196 /3а, б /
631 /ЛГ0006, 000263 /№634 /17.09.99 /17.09.2002 /Негосударственное образовательное учреждение «Академия «АйТи» /117218, Москва, ул. Кржижановского, 21 А, т. 974-7979, 974-7990 /6 /

**В ТАБЛИЦЕ ПРИНЯТЫ СЛЕДУЮЩИЕ ОБОЗНАЧЕНИЯ:**

**Перечень видов деятельности по защите информации, на которые выдана лицензия:**

1. Сертификация (1.1) и сертификационные испытания (1.2):
а) технических средств защиты информации;
б) защищенных технических средств обработки информации (ТСОИ);
в) технических средств контроля эффективности мер защиты информации;
г) программных средств защиты информации от НСД;
д) защищенных программных средств обработки информации от НСД;
е) программных средств контроля защищенности информации от НСД.
ж) программных средств по требованиям безопасности.
2. Контроль защищенности информации ограниченного доступа (2.1), аттестация средств и систем (2.2) на соответствие требованиям по защите информации:
а) автоматизированных системы различного уровня и назначения;
б) систем связи, приема, обработки и передачи данных;
в) систем отображения и размножения;
г) технических средств (систем), не обрабатывающих информацию ограниченного доступа, но размещенные в помещениях, где она обрабатывается;
д) помещений со средствами (системами), подлежащими защите;
е) помещений, предназначенных для ведения конфиденциальных переговоров.
3. Разработка (3.1), производство (3.2), реализация (3.3), установка (3.4), монтаж (3.5), наладка (3.6), испытания (3.7), ремонт (3.8) и сервисное обслуживание (3.9):
а) технических средств защиты информации;
б) защищенных ТСОИ;
в) технических средств контроля эффективности мер защиты информации;
г) программных средств защиты информации от НСД;
д) защищенных программных средств обработки информации от НСД;
е) программных средств контроля защищенности информации от НСД;
ж) программных средств по требованиям безопасности.
4. Проведение специсследований на ПЭМИН ТСОИ.
5. Проектирование объектов в защищенном исполнении:
а) автоматизированных систем различного уровня и назначения;

б) систем связи, приема, обработки и передачи данных;
в) систем отображения и размножения;
д) помещений со средствами (системами), подлежащими защите;
е) помещений, предназначенных для ведения конфиденциальных переговоров.
б. Подготовка и переподготовка кадров в области защиты информации по видам деятельности, перечисленным в данном перечне.
Дополнительно:
*) Бланк лицензии заменен при перелицензировании.
**) В части защиты конфиденциальной информации.

## Приложение 4

**ПЕРЕЧЕНЬ лицензионных центров в области защиты информация**

№ п/п /Наименование лицензионного центра (ведомственная принадлежность) /Адрес, телефон /Номер решения об аккредитации

1 /НИИ проблем автоматизации (Госкомсвязи России) /195272, С.-Петербург, пр. Шаумяна, 18, т. 164-17-97, 164-14-65 /Решение № 8а от 09.03.94 г.

2 /Научно-технический и сертификационный центр по комплексной защите информации "Атомзащитаинформ" (Минатом России) /101000, Москва, а/я 911, т. 239-22-62,239-47-28 /Решение № 11/01-1115 от 24.05.94 г.

3 /Центр безопасности программного обеспечения и новых информационных технологий при РВВКИУ РВ им. М.И. Неделина (Администрация Ростовской области и Ставропольского края) /344027, Ростов-на-Дону-27, РВВКИУ ракетных войск им. Главного Маршала артиллерии М. И. Неделина, т.31-84-00,31-84-15 /Решение № 39 от 26.08.96 г.

4 /5-й ЦНИИ Минобороны РФ (Гостехкомиссия России) /394052, Воронеж, ул. Краснознаменная, 153, т. 56-94-25,56-00-86 /Решение №21 от25.11.94г.

5 /Войсковая часть 96010 (Гостехкомиссия России) /103175, Москва, К-175, войсковая часть 96010, т. 293-01-77, 591-77-21 /Решение № 21 от 25.11.94г.

6 /Войсковая часть 54939 /Москва, войсковая часть 54939, т. 429-20-83 /Решение № 22 от25.11.94г.

7 /Войсковая часть 77111 (Минобороны РФ) /103160, Москва, К-160, войсковая часть 77111, т. 296-30-00, 296-30-01 /Решение № 23 от 25.11.94 г.

8 /Войсковая часть 55387 (Минобороны РФ) /103160, Москва, К-160, войсковая часть 55387, т, 293-66-38, 293-66-33 /Решение № 23 от 25.11.94 г.

9 /Московский региональный аналитический центр при Правительстве Москвы и администрации Московской области /103032, Москва, ул. Тверская, 13, т. 202-64-03, 288-74-10 /Решение №24 от 30.12.94 г.

10 /Войсковая часть 64829 (ФСБ России) /101000, Москва, войсковая часть 64829, т. 224-84-41,924-61-18, /Решение № 25 от30.12.94г.

11 /НИИ "Восход" (Госкомсвязи России) /119048. Москва, ул. Удальцова, 85, т. 931-92-52. 931-92-25 /Решение № 26 от 30.12.94 г.

12 /Центральный НИИ машиностроения (Российское космическое агентство) /141070, Калининград, Московской области, ул. Пионерская, 4, т. 516-33-35 /Решение № 27 от27.01.95г.

13 /НПО прикладной механики (Российское космическое агентство) /660026, Красноярск-26 Красноярского края, НПО прикладной механики, Т.(39197)28-

949/Решение № 27 от27.01.95г.

Продолжение приложения 4

№ п/п /Наименование лицензионного центра (ведомственная принадлежность) /Адрес, телефон /Номер решения об аккредитации

14 /Центр защиты информации «Норд» Государственного российского центра атомного судостроения (администрация Архангельской области) /164500, Северодвинск Архангельской обл., Архангельское ш., 58, т. 947-17, 946-01 /Решение №28 от 30.12.94 г.

15 /Российский центр «Безопасность» (Минэкономики) /103030, Москва, 1-й Семиловский пер., 16, т. 978-93-03, 978-91-55 /Решение № 29 от01.03.95г.

16 /Научно-технический и сертификационный центр «Заслон» (Минэкономики) /125833, Москва, Миусская пл., 3, т. 972-73-10, 251-25-22 /Решение № 30 от 26.04.95 г.

17 /Отраслевой отдел радиотехнических измерений при Государственном центральном научно-исследовательском радиотехническом институте (Минэкономики) /107066, Москва, ул. Новая Басманная, 20, т. 263-98-77,267-63-53 /Решение № 30 от 26.04.95 г.

18 /Пензенский научно-исследовательский электротехнический институт (Минэкономики) /440601, Пенза, ул. Советская, 9, т. (841-2) 66-39-06 /Решение № 30 от 26.04.95 г.

19 /АОЗТ «Кировский региональный центр деловой информации» (администрация Кировской области) /610005, Киров, ул. Мопра, 113, т. (8332) 62-49-36, 62-25-04 /Решение №31 от 30.06.95 г.

20 /Московский государственный инженерно-физический институт (Минобразования) /115409, Москва, Каширское ш., 31, т. 324-87-66, 324-84-32 /Решение № 32 от 30.06.95 г.

21 /Санкт-Петербургский государственный электротехнический университет (Минобразования) /197376, С.-Петербург, П-376, ул. Профессора Попова, 5, т. 237-59-84 /Решение № 32 от 30.06.95 г.

22 /Академия региональных проблем информатики и управления (Ассоциация экономического взаимодействия территорий Северо-Запада РФ) /193060, С.-Петербург, Смольный, 6-й проезд, т. 274-05-95, 274-89-86 /Решение № 33 от 23.10.95 г.

23 /НИИ специальной техники (МВД России) /101000, Москва, ул. Малая Лубянка, 16/4, т. 181-50-24,923-66-06 /Решение № 34 от 29.12.95 г.

24 /АОЗТ Научно-производственная фирма «Арго» (администрация Астраханской области) /414056, Астрахань, пер,. Смоляной, 2, т. 25-30-61,29-01-29 /Решение № 35 от 9.02.96 г.

25 /Концерн «Системпром» (АН) /107066. Москва, ул. Н. Красносельская, 13,корп.1, т. 267-20-31/Решение № 37 от 11.06.96г.

26 /Ассоциация документальной электросвязи (Госкомсвязи России) /117418, Москва, ул. Цюрупы, 1а, т. 123-63-44, 120-31-51 /Решение № 38 от 28.06.96 г.

27 /НИИ измерительных систем (администрация Нижегородской области) /603600. Н. Новгород, ГСП-486, НИИИС, т. 66-16-20, 65-49-90/Решение № 40 от 16.09.96г.

28 /ЗАО «Научно-производственный центр РИФ-ЗАЩИТА» (администрация Новосибирской области) /630075. Новосибирск, ул. Объединения, 3, т. 74-12-55,74-25-93/Решение №41 or25.10.96r.

Окончание приложения 4

№ п/п /Наименование лицензионного центра (ведомственная принадлежность) /Адрес, телефон /Номер решения об аккредитации

29 /Приморский региональный аналитический центр (администрация

Приморского края) /690090, Владивосток, ул. Алеутская, 45А, комн. 616, т. (4232) 260-736,217^75 /Решение № 45 от 02.06.97 г.

30 /Федеральное агентство информационной безопасности (Гостехкомиссия России) /141260, Красноармейск, Московская обл., ул. Центральная, 17 /Решение № 48 от ll.08.97 т.

31 /Региональный центр по защите информации и проведению специальных экспертиз (Кабинет Министров Республики Татарстан) /420029, Казань, ул. Журналистов, 50/3, т. (8432) 76-62-83, 76-77-15 /Постановление №451/690 от 10.09.97 г.

32 /АООТ «Амурская ЭРА» (Администрация Хабаровского края и Еврейской автономней области) /681000, Хабаровский край, Комсомольск-на-Амуре, Аллея Труда, 86, т. 4-51-10 - . /Решение № 42 от 11.02.98г.

33 /Калининградский государственный научно-исследовательский центр информационной и технической безопасности (администрация Калининградской области) /236007, Калининград, ул. Дм. Донского, 1, т. (0112) 46-54-09,46-46-43, 45-12-08 /№ 49 от 19.05.98 г.

34 /000 «СПУРТ Лтд.» (Российская академия естественных наук)/113405, Москва, Варшавское ш., 125 /№50 от l9.11.98 т.

## Приложение 5

**Перечень органов по аттестации системы сертификации средств защиты информации по требованиям безопасности информации Гостехкомиссии России**

№ п/п /Наименование предприятия — органа по аттестации объектов информатизации /Адрес регистрации /Номер аттестата /Срок действия аттестата

[1] /Государственное предприятие «Научно-технический центр «ЗАРА» /125889, Москва, Миусская пл., 3 /СЗИ RU. 167. В21.001 /22.07.97/ 22.07.2001

2 /Центр безопасности программного обеспечения и новых информационных технологий Ростовского ВВКИУ РВ /344027, Ростов-на-Дону-27, пр. Октября, 24/50 /СЗИ RU. 018. В31.002 /05.10.97/ 05.10.2001

3 /Государственное унитарное предприятие специализированный центр программных систем «СПЕКТР» /197342, Санкт-Петербург, ул. Кантемировская, 10 /СЗИ RU. 336. В22.003 /09.10.97/ 09.10.2001

4 /АОЗТ «Многопрофильное внедренческое предприятие «СВЕМЕЛ» /109028, Москва, Серебрянический пер.,5, стр.2 /СЗИ RU. 057. В01.004 /20.11.97/ 20.11.2001

5 /Центр безопасности информации /141080, Юбилейный Московской обл., ул. Тихонравова, 34, 4-й ЦНИИ МО /СЗИ RU. 117. В02.005 /20.11.97/ 20.11.2001

б /Научно-техническая и конструкторская фирма «Информационная гидроакустика» /194044, Санкт-Петербург, ул. Кантемировская, 4 /СЗИ RU. 346. В03.006 /20.11.97/ 20.11.2001

7 /Пензенский филиал НТЦ «Атлас» ФАПСИ /440601, Пенза, ул. Советская, 9 /СЗИ RU. 085. В61.007 /29.12.97/ 29.12.2001

8 /АОЗТ «РНТ» /111141, Москва, 2-й проезд Перова поля, 9 /СЗИ RU. 003. В04.00& /26.01.98/ 26.01.2002

9 /ГНПП «Информакустика» /197136, С.-Петербург, Чкаловский пр., 50 /СЗИ RU. 076. В23.009 /26.01.98/ 26.01.2002

10 /Центральный научно-исследовательский институт управления, экономики и информации (ЦНИИАТОМИНФОРМ) Минатома России /127434, Москва,

Дмитровское ш., 2 /СЗИ RU. 004. В11.010 /25.02.98/ 25.02.2002
11 /5-й ЦНИИ МО РФ /394052, Воронеж, ул. Краснознаменная, 153 /СЗИ RU. 005. В32.011 /08.04.98/ 08.04.2002
12 /ИЦС и А «Безопасные информационные технологии»(«Бинтех») /394036, Воронеж, ул. Студенческая, 36 /СЗИ RU. 073. В05.012 /08.04.98/ 08.04.2002
13 /ООО «Кировский региональный центр деловой информации» /610005, Киров, ул. Мопра, 113 /СЗИ RU. 058. В06.013 /27.05.98/ 27.05.2002
14 /Государственное унитарное предприятие «Специальное агентство экспертизы, лицензирования, сертификации и аттестации «Омега» /195220, Санкт-Петербург, ул. Обручевых, 1 /СЗИ RU. 224. В07.014 /30.04.98/ 30.04.2002
15 /Общественное объединение «Ассоциация документальной электросвязи» /103375. Москва, ул. Тверская, 7 /СЗИРи.345 В07.015 /12.05.98/ 12.05.2002
16 /ОАО «ОПТИМА» /107082, Москва, Рубцовская наб., 3 /С3HRU.340 В08.016 /22.05.98/ 22.05.2002
17 /ООО «Монтажно-технологическое управление «ТЕЛЕКОМ-С» /355044, Ставрополь, пр. Кулакова,5-1Г /СЗИ RU. 319.В09.017 /22.05.98/ 22.05.2002
18 /Специальный центр МЧС России /103012, Москва, Театральный проезд, 3 /С3HRU.001. В41.018 /3.09.98/ 3.09.2002
Продолжение приложения 5
№ п/п /Наименование предприятия — органа по аттестации объектов информатизации /Адрес регистрации /Номер аттестата /Срок действия аттестата
19 /НТЦ «Критические информационные технологии» /196135, Санкт-Петербург, ул. Гастелло, 16 /С3HRU.77. В010.019 /22.06.98/ 26.06.2002
20 /НТиСЦ «Заслон» /125833, Москва, Миусская пл., 3 /СЗИ RU. 115 В25.020 /3.09.98/ 3.09.2002
21 /ЦКБИ ГУП СНПО «Элерон» /115563, Москва, ул. Генерала Белова, 14 /СЗИ RU.069. В12.21 /3.09.98/ 3.09.2002
22 /ООО «Центр безопасности информации «Маском» /117571, Москва, пр. Вернадского, 86, корп. б, комн.119 /СЗИ RU.094. ВОН.022 /30.09.98/ 30.09.2002
23 /ОАО «НОВО» /127434, Москва, ул. Дубки, 6 /СЗИ RU.062. В012.023 /30.11.98/ 30.11.2002
24 /ТОО «Александр» /129110, Москва, ул. Средняя Переяславская, 27,стр.1 /СЗИ RU.075. В013.024 /14.10.98/ 14.10.2002
25 /РЦ «Безопасность» /129626, Москва, ул. Проспект Мира, 102 /СЗИ RU.114. В026.025 /27.10.98/ 27.10.2002
26 /НПО прикладной механики /660033, Железногорск Красноярского края, пр. Ленина, 52 /СЗИ RU.011. В27.026 /14.10.98/ 14.10.2002
27 /НТиСЦ «Атомзащитаинформ» /101000, Москва, ул. Большая Ордынка, 24/26 /СЗИ RU.002. В 12.027 /6.11.98/ 6.11.2002
28 /ЦНИИЭИСУ /103104, Москва, Тверской бульвар,7/2 /СЗИ RU.400. В28.028 /25.11.98/ 25.11.2002
29 /ООО «Научно-производственная лаборатория «ИНФО-КРИПТ 2000» /117419, Москва, ул. Шаболовка, 50 /СЗИ RU.503. В014.029 /25.11.98/ 25.11.2002
30 /ООО «Конфидент» /193184, Санкт-Петербург, Большой Смоленский пер., 36 /СЗИ RU.524. В015.030 /25.11.98/ 25.11.2002
31 /ООО «Аттестационный центр «Ветеран» /117418, Москва, ул. Цурюпы, 14 /СЗИ RU.237. ВО 16.031 /27.11.98/ 27.11.2002
32 /ОАО «ОКБ «Карат» /644065, Омск, пос. Первомайский, 2 /СЗИ RU.477.

B017.032 /27.11.98/ 27.11.2002

33 /ЗАО «Лаборатория противодействия промышленному шпионажу» (Лаборатория ППШ) /190000, Санкт-Петербург, пер. Гривцова, 1/64 /СЗИ RU.054. B019.034 /8.12.98/ 8.12.2002

34 /Краснодарский филиал государственного унитарного предприятия «Научно-технический центр «Атлас» /350068, Краснодар, ул. Красноармейская, 20 /СЗИ RU. 183. B91.035 /9.12.98/ 9.12.2002

35 /Государственное учреждение «Калининградский государственный научно-исследовательский центр информационной и технической безопасности» /236007, Калининград, ул. Дм. Донского, 1 /СЗИ RU.523. B92.036 /11.12.98/ 11.12.2002

36 /Военный институт радиоэлектроники Министерства обороны РФ /394020, Воронеж, ул. Краснознаменная, 153 /СЗИ RU.326. B33.037 /22.12.98/ 22.12.2002

37 /Региональный центр по защите информация и проведению специальных экспертиз /420029, Казань, ул. Халитова, 3 /СЗИ RU.434. B93.038 /12.01.99/ 12.01.2003

38 /000 «Центр технических средств защиты информации» /620014. Екатеринбург, ул. Хохрякова, 87, кв.509 /СЗИК.и.531. B020.039 /15.01.99/ 15.01.2003

Окончание приложения 5

Ms п/п /Наименование предприятия — органа по аттестации объектов информатизации /Адрес регистрации /Номер аттестата /Срок действия аттестата

39 /Научно-производственное государственное предприятие «Гамма» /117420, Москва, ул. Профсоюзная, 78. /СЗИ RU.082. B029.040 /03.02.99/ 03.02.2003

40 /Государственное предприятие «Омский научно-исследовательский институт приборостроения» /644009, Омск, ул. Масленникова, 231 /СЗИ RU.452. B021.041 /12.02.99/ 12.02.2003

41 /НИЦИ при МИД России /119021, Москва, ул. Остоженка, 53/2, /СЗИ RU. B94.042 /18.02.99/ 18.02.2003

42 /ЗАО «Научно-техническая фирма «КРИПТОН» НИИАА» /117420, Москва, ул. Профсоюзная, 78 /СЗИ RU.059. B022.043 /19.02.99/ 19.02.2003

43 /ЗАО «АйТи». Информационные технологии» /103575, Москва, Зеленоград, корп.1003, пом.РЭУ /СЗИ RU.275. B023.044 /31.03.99/ 31.03.2003

44 /ЗАО «Производственная организация вычислительной техники и средств автоматизации»/113425, Москва, Варшавское ш., 125 /СЗИ RU.440. B024.045 /8.04.99/ 8.04.2003

## Приложение 6

**Перечень органов по сертификации системы сертификации средств защиты информации по требованиям безопасности информации Гостехкомиссии России**

№ п/п /Наименование предприятия — органа по сертификации /Адрес регистрации /Номер аттестата /Срок действия аттестата

/Научно-технический и сертификационный центр по комплексной защите информации «Атомзащитаинформ» при Минатоме России. /101000, Москва ул. Большая Ордынка, 24/26 /СЗИ RU.002. АН.002 /23.01.96/ 23.01.2000

2 /5-й ЦНИИ МО РФ /394052, Воронеж, ул. Краснознаменная, 153 /СЗИ RU. 005. A31.003 /23.04.96/ 23.04.2000

3 /АОЗТ НТЦ «Критические информационные технологии» /196135, Санкт-Петербург, ул. Гастелло, 16 /СЗИ RU.77. А01.004 /26.06.96/ 26.06.2000

4 /Секция «Информационная безопасность» Российской инженерной академии /103905, Москва, ул. Тверская,11 /СЗИ RU.341. А91.005 /17.07.97/ 17.07.2001

5 /Общественное объединение «Ассоциация документальной электросвязи» /103375, Москва, ул. Тверская, 7 /СЗИ RU.345 А02.006 /12.05.98/ 12.05.2002

## Приложение 7

**Перечень испытательных лабораторий системы сертификации средств защиты информации по требованиям безопасности информации Гостехкомиссии России**

№ п/п /Наименование предприятия — испытательной лаборатории по сертификации /Адрес регистрации /Номер аттестата /Срок действия аттестата

1 /Центр комплексной безопасности информации государственного предприятия СНПО «Элерон» /115563, Москва, ул. Генерала Белова, 14 /СЗИ RU. 069. Б11.001 /6.03.96/ 6.03.2000

2 /АОЗТ «Лаборатория противодействия промышленному шпионажу» (Лаборатория ППШ) /190000, Санкт-Петербург, 1/64 /СЗИ RU. 054.БО 1.002 /6.03.96/ 6.03.2000

3 /Центральный научно-исследовательский институт управления, экономики и м информации (ЦНИИАТОМИНФОРМ) Минатом России /127434, Москва, Дмитровское ш., 2 /СЗИ RU. 004.Б12. 903 /26.03.96/ 26.03.2000

4 /АОЗТ «РНТ» /127434, Москва, а/я 971 /СЗИ RU. 003. Б02. 004 /11.04.96/ 11.04.2000

5 /Войсковая часть 11135 /103160, Москва, К-160 /СЗИ RU. 105. Б31. 005. /19.04.96/ 19.04.2000

6 /5-й ЦНИИ МО РФ /394052, Воронеж, ул. Краснознаменная, 153 /СЗИ RU. 005.Б32.006 /23.04.96/ 23.04.2000

7 /Войсковая часть 52195 (специальный центр МЧС России) /121352, Москва, ул. Давыдковская, 7А /СЗИ RU. 001.Б41.007 /04.06.96/ 04.06.2000

8 /ГНПП «Информакустика» /197136, Санкт-Петербург, Чкаловский пр., 50 /СЗИ RU. 076. Б21.008 /11.06.96/ 11.06.2000

9 /ЦФТИМОРФ /141300, Сергисв-Посад, Московской обл. /СЗИ RU. 125.Б33.009 /02.07.96/ 02.07.2000

10 /Войсковая часть 30895 /198903,Санкт-Петсрбург, Петродворец, ул. Разводная, 17 /СЗИ RU. 031.Б34.010 /08.07.96/ 08.07.2000

11 /Войсковая часть 01168 /123007, Москва, 1-и Хорошевский проезд, 5 /СЗИ RU. 102.Б35.011 /08.07.96/ 08.07.2000

12 /ИЦСиА «Безопасные информационные технологии»(«Бинтех») /394036, Воронеж, ул. Студенческая, 36 /СЗИ RU. 073.Б03.012 /08.07.96/ 08.07.2000

13 /МРАЦ /103032, Москва, ул. Тверская, 13, /СЗИ RU. 052.Б04.013 /30.07.96/ 30.07.2000

14 /НПФ «ПРОМТЕХН» /121471,Москва, Можайское ш., 29/2 /СЗИ RU. 007.Б05.014 /08.07.96/ 08.07.2000

15 /Центр безопасности программного обеспечения и новых информационных технологий Ростовского ВВКИУ РВ /344027, Ростов-на-До-ну-27, пр. Октября, 24/50 /СЗИ RU. 018.Б03.015 /08.07.96/ 08.07.2000

16 /Войсковая часть 64829 /101000, Москва, ул. Мясницкая, 3/6 /СЗИ RU. 110. Б51.016 /25.07.96/ 25.07.2000

17 /Войсковая часть 49456 /125284, Москва, Хорошевское ш., 38А /СЗИ RU. 098.Б37.017 /16.08.96/ 16.08.2000

18 /Малое государственное внедренческое научно-производственное предприятие «Спектр» Института теоретической и экспериментальной физики Минатома России /117259, Москва, ул. Б.Черемушкинская, 25 /СЗИ RU. 012.Б13.018 /10.12.96/ 10.12.2000

Окончание приложения 7

№ п/п /Наименование предприятия —испытательной лаборатории по сертификации /Адрес регистрации /Номер аттестата /Срок действия аттестата

19 /Научно-технический центр «Критические информационные технологии» /196135, Санкт-Петербург, ул. Гастелло, 16 /СЗИ RU. 077. Б06.019 /26.12.96/ 26.12.2000

20 /Научно-исследовательская лаборатория «ЭЛКО» ГЦИПК Минатома России /294020, Обнинск Калужской обл, ул. Курчатова, 21 /СЗИ RU. 072.Б14.020 /27.12.96/ 27.12.2000

21 /Государственное унитарное предприятие Специализированный центр программных систем «Спектр» /197342, Санкт-Петербург, ул. Кантемировская, 10 /СЗИ RU. 189.Б22.021 /3.4.97/ 3.4.2001

22 /ЗАО «Документальные системы-МФД» /123557, Москва, Электрический пер., 3 /сзири. 304. Б07. 022 /11.4.97/ 11.4.2001

23 /ВИКА им. А.Ф. Можайского /197082, Санкт-Петербург, Ждановская наб., 13 /СЗИ RU. 030. Б37.023 /25.4.97/ 25.4.2001

24 /НИИ автоматики /127106, Москва, ул. Ботаническая, 25 /СЗИ RU. 076. Б23.024 /22.5.97/ 22.5.2001

25 /Центр безопасности информации /141080, Юбилейный, Московской обл., ул. Тихонравова, 34, 4-й ЦНИИ МО /СЗИ RU. 117. Б08.025 /23.5.97/ 23.5.2001

26 /РЦ «Безопасность» /109316, Москва, Волгоградский пр., 16 /СЗИ RU. 114. Б24.026 /3.6.97/ 3.6.2001

27 /Пензенский филиал НТЦ «Атлас» ФАПСИ /440601, Пенза, ул. Советская, 9 /СЗИ RU. 085. Б61.027 /15.7.97/ 15.7.2001

28 /Научно-техническая и конструкторская фирма «Информационная гидроакустика» /194044, Санкт-Петербург, ул. Кантемировская, 4 /СЗИ RU. 346. Б08. 028 /15.7.97/ 15.7.2001

29 /Войсковая часть 77111 /103160, Москва, К-160 /СЗИ RU. 174. Б38. 029 /21.8.97/ 21.8.2001

30 /ЗАО «НПО «КРИПТОН» /123424, Москва, Волоколамское ш., 90 /СЗИ RU. 307. БОЮ. 030 /9.10.97/ 9.10.2001

31 /ЗАО «Лаборатория новых информационных технологий «ЛАНИТ» /107066, Москва, ул. Доброслободская, 5 /СЗИ RU. 309.Б011.031 /3.11.97/ 3.11.2001

32 /Испытательный центр ЗАО «Анкей/Холдинг» /113114, Москва, ул. Летниковская, 4, стр.5 /СЗИ RU. 390.Б012.032 /22.05.98/ 22.05.2002

33 /000 «Монтажно-технологическое управление «ТЕЛЕКОМ-С» /355044, Ставрополь, пр. Кулакова, 5-1 Г /СЗИ RU. 319.Б013.033 /22.05.98/ 22.05.2002

34 /Государственное унитарное предприятие «Специальное агентство экспертизы, лицензирования, сертификации и аттестации «Омега» /195220, Санкт-Петербург, ул. Обручевых, 1 /СЗИ RU. 224.Б25. 034 /10.07.98/ 10.07.2002

35 /ЗАО «Микротест» /620027, Екатеринбург, ул. Челюскинцев, 70/30 /СЗИ

RU. 509.Б014.036 /19.10.98/ 19.10.2002

36 /000 «АйСиЭс» /125047, Москва, ул. 4-я Тверская-Ямская, 26/8, стр.1 /СЗИ RU. ЗО3.Б015.037 /17.11.98/ 17.11.2002

37 /НИИ радио /103064, Москва, ул. Козакова,16 /СЗИ RU. 061.Б91.038 /30.11.98/ 30.11.2002

38 /Федеральное унитарное предприятие «Научно-производственное объединение прикладной механики» /660033, Железногорск Красноярского края, Ленина, 52 /СЗИ RU. 011.Б27.039 /12.01.99/ 12.01.2003

## Приложение 8

**ПЕРЕЧЕНЬ средств защиты информации, сертифицированных по требованиям безопасности информации РОСС RU. 0001. 01БИОО**

№ п/п /Регистрационный номер сертификата /Дата внесения в государственный реестр /Срок действия сертификата /Наименование средства (шифр) /Предназначение средства (область применения), краткая характеристика параметров /Тип средства /Заявитель

1 /1 /23.12.93 / /«Снег 1.0» /Система защиты информации от НСД «Снег 1.0» для ПЭВМ ЮМ РС XT/AT, под управлением ОС MS DOS 3.30,4.01,5.0 — по классу 1Б для АС. В состав входит СКЗД «Иней» /Серия ПТ(СМ.Сноску 1) /ЦНИИ Атоминформ Минатома России

2 /4 /09.11.93 /23.12.2001 / /Встроенная система парольной защиты загрузки ПЭВМ PCD-4 Gsx/25 фирмы Simens Nixdorf/ПТ /Управление информационных ресурсов Администрации Президента РФ

3 /6 /23.12.93 г. /23.12.2001 /«Снег-ЛВС» /1. Система защиты информации от НСД в ЛВС «Снег-ЛВС» под управлением Advanced/SFT NetWare 2/xx, NetWare 386 3/xx Исполнение 1 — в состав входит СКЗД «Иней» и «Иней-ЛВС» —по классу 1Б для АС Исполнение 2 — без СКЗД «Иней» и «Иней-ЛВС» — по классу 1 В для АС 2. Система защиты информации от НСД в ПЭВМ «Снег 1.0» под управлением MS DOS 5.0,6.0 Исполнение 1 — в состав входит СКЗД «Иней» — по классу 1 Б для АС Исполнение 2— без СКЗД«Иней»— поювосу1В для АС Все устройства — по классу 3 для СВТ/ПТ Серия /ЦНИИ Атоминформ Минатома России

4 /16 /15.02.96 /15.02.2002 /ГШ—1000 /Средство активной защиты — генератор шума ГШ-1000 с диапазоном частот от 0,1 до 1000МГц—на соответствие ТУ /Т Серия /ЦНИИМАШ РКА СКБИРЭ РАН

___

Сноска 1. ПТ (ПА) — программно-технические (программно-аппаратные) средства защиты информации;
Т — технические средства защиты информации;
П — программные средства защиты информации.

___

Продолжение приложения 8

№ и/а /Регистрационный номер сертификата /Дата внесения в государственный реестр /Срок действия сертификата /Наименование средства (шифр) /Предназначение средства (область применения), краткая характеристика параметров /Тип средства /Заявитель

5 /17 /27.09.95 /31.12.2001 /ФСПК-200(100) /Защитное устройство—фильтр сетевой помехоподавляющий комбинированный ФСПК-100 (200) — на соответствие требованиям нормативных документов /Т Серия /ГЦИПК НПП «Элком»

6 /21 /31.12.95 /31.12.2001 /«Страж I.I» /Программный комплекс защиты

информации от НСД «Страж 1.1» для ПЭВМ—по классу 2 для СВТ /П /в/ч 01168

7 /22 /10.11.95 /31.12,98 /«Марс» /Комплекс программных средств зашиты от НСД для персонального компьютера «Марс» (КПСЗИ «Марс») — по классу защищенности 3 /П /Российский центр «Безопасность»

8 /25 /25.12.95 /31.12.2001 /ГШ-К-1000 /Средство активной защиты — генератор шума ГШ-К-1000 с диапазоном частот от 0,1 до 1000 МГц — на соответствие ТУ /Т Серия /СКБИРЭРАН

9 /26 /25.12.95 /31.12.2001 /«Салют» /Изделие «Салют» для защиты ПЭВМ от перехвата ЭМИиН объектов ВТ категорий 2,3 в диапазоне частот 10—1000 МГц — на соответствие норм. документов Гостехкомиссии России по защите от утечки за счет ПЭМИН /Т Серия /ТОО «НТФ «Криптон»

10 /27 /25.12.95 /31.12.2001 /«Корунд» /Устройство защиты от прослушивания речевой информации через ТА в режиме ожидания вызова (РА0019301 ТУ) /Т Серия /ТОО«РЕНОМ»

11 /32 /20.04.96 /20.04.99 /«СНЕГ 2.0» /Программное средство защиты информации от НСД в автоматизированных системах на базе автономной ПЭВМ с ОС MS DOS версий 5.0 и 6.22 — по классу защищенности 1 Б; по классу защищенности 2 — в средствах вычислительной техники (сертифицированных) /П /ЦНИИ Атоминформ

12 /33 /18.04.96 /31.12.99 /ЭКР4110Ф /Электронная контрольно-кассовая машина ЭКР4110 Ф — по группе 2 для ККМ и классу 6 для СВТ /ПТ Серия /Курское АОЗТ «Счетмаш»

13 /34 /29.04.96 /29.04.99 /«Аккорд» /Программно-аппаратный комплекс «Аккорд» (версия ПО и БИОС 1.31/1.10) по классу 1Д (для произвольной программной среды ПЭВМ) и по классу 1В (для функционально-замкнутой программной среды ПЭВМ) для АСУ/ПТ Серия /ОКБ САПР ТОО «Фирма «Информкриш» Лтд.»

Продолжение приложения 8

№ п/п /Регистрационный номер сертификата /Дата внесения в государственный реестр /Срок действия сертификата /Наименование средства (шифр) /Предназначение средства (область применения), краткая характеристика параметров /Тип средства /Заявитель

14 /35 /06.05.96 /06.05.99 /«OMRON FIT GR-25 RF» /Контрольно-кассовая машина «OMRON FIT GR-25 RF» — по группе 1 класса 1 для ККМ /ПТ 1000 эк3. /СП «РИТ»

15 /36 /22.05.96 /22.05.99 /«SVET&Q» /Программно-аппаратный комплекс защиты информации в автоматизированных системах от НСД — по классу защищенности 1 В; по классу защищенности 4 — для сертифицированных СВТ /ПТ /ГНИ ВЦ Государственного таможенного комитета, ОКБ САПР

16 /37 /22.05.96 /22.05.99 /«ДИЗ 1.0» /Программно-аппаратное средство защиты информации от НСД в локальных вычислительных сетях Novel Netware (v.3.11) и на автономных АРМ на базе ПЭВМ IBM PS/AT с ОС MS DOS версий 3.30 и выше — по классу защищенности 2 <s /ПТ Серия /в/ч 49456

17 /38 /22.05.96 /22.05.99 /«SECRET NETv.2.1» /Программно-аппаратный комплекс (сетевой и автономный вариант) защиты информации от НСД в ЛВС Novel Netware (v.3.11), Windows for Workgroups (v.3.11) с использованием ОС MS DOS (V.3.3-7.0), PS DOS (V.3.30-6.30) — по классам защищенности ЗА, 2Б, 1 В для АС и классу защищенности 3 для сертифицированных СВТ /ПТ /ЗАО НИЛ «Информзащита»

18 /39 /26.06.96 /26.06.99 / /Программно-аппаратное средство защиты от НСД фискальных данных контрольно-кассовых машин «Спектр-001 ф» и «IBC POS II S» — по группе 2 класса 2 для ККМ /ПТ Серия /АОНИИВС «Спектр»

19 /40 /26.06.96 /26.06.99 / /Средство защиты информации от НСД

«Менеджер элементов системы управления TN-MS 1.3» в автоматизированной системе управления сетью «Метроком» при применении с операционной средой UNIX — по классу защищенности 1Г для АСУ/П /АОЗТ «Метроком»
Продолжение приложения 8
№ п/п /Регистрационный номер сертификата /Дата внесения в государственный реестр /Срок действия сертификата /Наименование средства (шифр) /Предназначение средства (область применения), краткая характеристика параметров /Тип средства /Заявитель
20 /41 /30.07.96 /30.07.99 /«Гром-ЗИ-4» /Генератор шума «Гром-ЗИ-4» с излучателем DA3000 — для маскировки ПЭМИ ПЭВМ, ЛВС на базе ПЭВМ путем создания активных помех в диапазоне 20— 1000 МГц, соответствует требованиям САЗ объектов ЭВТ от утечки информации по ПЭМИН, осн. требованиям (Минрадиопром,1987) и требованиям ТУ на генератор шума «Гром-ЗИ-4»; создания помех в сети электропитания и в телефонной линии, соответствует требованиям ТУ на ГШ «Гром-ЗИ-4» /Т Серия /АОЗТ «Защита информации»
21 /42 /30.07.96 /30.07.99 /«Гром-ЗИ-6» /Генератор шума «Гром-ЗИ-6»— для генерации сигнала в сети электропитания и генерации сигналов в телефонной линии, соответствует требованиям ТУ на ГШ «Гром-ЗИ-6»/Т Серия /АОЗТ «Зашита информации»
22 /43 /18.07.96 i. /18.07.99 / /Комплекс средств защиты системы документальной связи компьютерной сети Тульской области — по классу 2Б для АС /П /Администрация Тульской области
23 /44 /22.07.96 /22.07.99 /— /Персональные ЭВМ PC/AT /Т /Московский индустриальный банк
24 /45 /30.07.96 /30.07.99 /«Коннекс» /Учрежденческая АТС типа «Коннекс» модели М7 — по «Нормам эффективности защиты технических средств передачи речевой, телеграфной и телекодовой информации от утечки за счет ПЭМИН», по «Нормам эффективности защиты АСУ и ЭВТ от утечки за счет ПЭМИН» — для объектов категории 3, по РД СВТ — по классу 7 (защита от НСД) /т Серия /ГП НИИ «Рубин»
25 /46 /30.07.96 /30.07.99 /«SKIP» /Программный продукт «SKIP» для регулирования доступа на интерфейсе «локальная/глобальная сеть» под управлением ОС Windows 3.11 и Windows 95, соответствует ТУ и классу защищенности ЗБ — для АСУ/П /АОЗТ«Элвис+»
26 /47 /26.08.96 /26.08.99 /X-Ring SP /Персональные ЭВМ типа PC/AT (торговая марка «X-Ring SP») — по «Нормам эф. защиты АСУ И СВТ от утечки за счет ПЭМИН» — для объектов категории 2/Т /ЗАО «Икс-Ринг Техно»
Продолжение приложения 8
№ п/п /Регистрационный номер сертификата /Дата внесения в государственный реестр /Срок действия сертификата /Наименование средства (шифр) /Предназначение средства (область применения), краткая характеристика параметров /Тип средства /Заявитель
27 /48 /26.08.96 /26.08.99 /«SKIP» /Программный продукт «SKIP» для регулирования доступа на интерфейсе «локальная/глобальная сеть» под управлением ОС Solaris 2.4, соответствует ТУ и классу защищенности ЗБ — для АСУ /П /АОЗТ «Элвис+»
28 /49 . /12.09.96 /12.09.99 /«Инфотекс» /Программное обеспечение корпоративной наложенной сети для удаленной защищенной связи «Инфотекс», соответствует классу защищенности 1В—для АСУ /П /ОАО «Инфотекс»
29 /50 /12.09.96 /12.09.99 /«Voice Coder» /Программные и технические средства телефонного аппарата Voice Coder-2400 соответствуют классу 6 — для СВТ /ПТ Серия /ЗАО «Сигнал-Ком»

30 /51 /25.09.96 /25.09.99 /«Шериф» /Программное средство защиты информации от НСД «Система защиты информации «Шериф» /П /ГНПО «Марс» Производственный кооператив «Биотекс»

31 /52 /3.10.96 /3.10.99 / /Партия ККМ «ABS POS Terminal System IIRF» с заводскими № 410600—411600 включительно — по группе 2 класса 2 для ККМ /ПТ 1000 экз. /ТОО «Синт Лтд.»

32 /53 /6.10.96 /6.10.99 /— /Детектор электромагнитного поля D006 /Т Серия /АОЗТ«Смерш Техникс»

33 /55 /15.11.96 /15.11.99 /«Банк-Клиент» /Средства защиты информации от НСД автоматизированной системы пересылки документов «Банк-Клиент» /П /ТОО «Инист»

34 /56 /1.11.96 /1.11.99 / /Средства защиты информации программного обеспечения Торгово-депозитарной расчетной системы Московской межбанковской валютной биржи — по классу 1 Г для АСУ /ПТ /ЗАО «Московская межбанковская валютная биржа»

35 /57 /25.12.96 /25.12.99 /«Смог» /Устройство защиты «Смог» в совокупности с антенной системой в диапазоне частот от 0,005 до 1000МГц /т Серия /НЛП «Союз»

36 /58 /14.11.96 /14.11.99 / /Средства защиты от НСД к информации фискальной памяти ККМ типа «Sharp ER-A250RB> — по группе 1 класса 2 для ККМ /ПТ /АОЗТ «УЭБ Текнолоджи»

Продолжение приложения 8

№ п/п /Регистрационный номер сертификата /Дата внесения в государственный реестр /Срок действия сертификата /Наименование средства (шифр) /Предназначение средства (область применения), краткая характеристика параметров /Тип средства /Заявитель

37 /59 /19.11.96 /19.11.99 /«Линтер» /Система управления базами данных «Линтер» версии 4.3 соответствует классу защищенности 5— для СВТ /П /ВНИИНС

38 /60 /3.12.96 /3.12.99 /«Виконт» /Технические средства видеоконтроля телевизионной системы наблюдения «Виконт» /Т Серия /НПО «Альфа-Прибор»

39 /61 /3.12.96 /3.12.99 / /Зонд-монитор СРМ-700 для индикации и контроля электромагнитных излучений в диапазоне от 50 кГц до 3 ГГц — соответствует техническим условиям АОЗИ.318231.017ТУ /Т Серия /АОЗТ «Защита информации»

40 /62 /14.12.96 /14.12.99 / /ПЭВМ IBM PC 330 зав № 554F1GO и ПЭВМ ЮМ РС 350 зав № 559H3L7 в диапазоне частот от 0,015 до 1000 МГц для объектов ЭВТ категории 3 (контролируемая зона — не менее 11 метров) /Т 2 экз. /Главное управление Центрального Банка РФ по г. Владимиру

41 /63 /20.12.96 /20.12.99 /— /Изделия ИКСГ.101, ИКСГ.102, ИКСГ.103 /П /АООТ НИИ ЦСУ «Экор»

42 /64 /23.12.96 /23.12.99 /«Лабиринт» /Аппаратно-программный комплекс «Система защиты информации на ПЭВМ» (шифр «Лабиринт») /ПТ Серия /НИИ «Центрпрограммсистем»

43 /65 /24.12.96 /24.12.99 / /Операционная система МС ВС /П /ВНИИ автоматизации управления в непромышленной сфере

44 /66 /26.12.96 /26.12.99 /«Волна-4М» /Устройство активной защиты информации «Волна-4М» в диапазоне частот от 100 кГц до 1000 МГц для объектов категории 2 и 3 /Т Серия /ЦКБИГПСНПО «Элерон»

45 /67 /26.12.96 /26.12.99 /«Сигнал-3» /Устройство защиты телефонных линий «Сигнал-3» для выделенных помещений категорий 1,2,3 /Т Серия /Тоже

46 /68 /26.12.96 /26.12.99 /«Сигнал-5» /Устройство защиты телефонных линий «Сигнал-5» для выделенных помещений категорий 1,2,3 /Т Серия /« «

47 /69 /26.12.96 /26.12.99 /«Сигнал-7» /Устройство защиты телефонных линий «Сигнал-7» для выделенных помещений категорий 1,2,3 для объектов категории 1 /Т Серия /« «

Продолжение приложения 8

№ п/п /Регистрационный номер сертификата /Дата внесения в государственный реестр /Срок действия сертификата /Наименование средства (шифр) /Предназначение средства (область применения), краткая характеристика параметров /Тип средства /Заявитель

48 /70 /26.12.96 /26.12.99 /«Кабинет» /Система акустической и вибрационной защиты «Кабинет» — на соответствие ТУ /Т Серия /ЦКБИГПСНПО «Элерон»

49 /71 /26.12.96 /26.12.99 /«Волна-ЗМД» /Устройство активной защиты информации «Волна-ЗМД» в диапазоне частот от 100 кГц до 1000 МГц для объектов категории 2 и 3 /Т Серия /Тоже

50 /72 /10.01.97 /10.01.2000 /«Пелена-3» /Изделие «Пелена-3» в диапазоне от 20 до 500 МГц — на соответствие ТУ /Т Серия /АОЗТ «Кобра»

51 /73 /16.01.97 /16.01.2000 /«Пандора» /СЗИ от НСД в сетях передачи данных по протоколу TCP/IP — межсетевой экран «Пандора» — по классу защищенности ЗБ для АСУ /МЭ[1] /АО «Релком-Альфа»

52 /74 /23.01.97 /23.01.2000 /«Грань-300» /Устройство защиты «Грань-300» для защиты телефонных аппаратов от перехвата речевой акустической информации при положенной на рычаг телефона трубке — на соответствие ТУ /Т Серия /000 «Паланге

53 /75 /23.01.97 /23.01.2000 /«УЗТ» /Устройство защиты «УЗТ» для защиты телефонных аппаратов от перехвата речевой акустической информации при положенной на рычаг телефона трубке — на соответствие ТУ /Т Серия /ТОО «Предприятие ЛиК»

54 /76 /27.01.97 /27.01.2000 /«Редут» /Программно-аппаратный комплекс защиты ПЭВМ от НСД «Редут» — по классу защищенности 5 для СВТ /ПТ 30 экз. /000«Анкей»

55 /77 /30.01.97 /30.01.2000 /-/Средства защиты информации от НСД, встроенные в программное обеспечение «Модуль оператора цифровой автоматической телефонной станции ЭЛКОМ» — по классу 3 для АСУ /П /Акционерная Русская Телефонная Компания

56 /78 /30.01.97 /30.01.2000 /-/Система защиты информации автоматизированной системы управления маршрутизатором фирмы Cisco серии 2500 (серийные № 25466922 — 25466951) /П 30 экз. /ЗАО «Релком-Альфа»

[1] МЭ - межсетевой экран.

Продолжение приложения 8

№ п/п /Регистрационный номер сертификата /Дата внесения в государственный реестр /Срок действия сертификата /Наименование средства (шифр) /Предназначение средства (область применения), краткая характеристика параметров /Тип средства /Заявитель

57 /79 /30.01.97 /30.01.2000 /Black Hole /Автоматизированная система разграничения доступа Black Hole версии BSDI- OS (серийные № 1-30— 30-30) — по классу ЗБ для АСУ /ПТ 30 экз. /ЗАО «Релком-Альфа»

58 /80 /30.01.97 /30.01.2000 /Secret Net /Система защиты Secret Net версии 3.0 (серийные № 1-100—100-100)—под управлением Windows 95 на рабочих станциях и сетевой ОС Novell Net Ware версии 3.11-4.1 на файл-сервере — по классу 3 для СВТ /П 100 экз. /ЗАО «Научно-инженерное предприятие «Информзащита»

59 /81 /4.03.97 /4.03.2000 /OSC-5000 /Омни-спектральный коррелятор OSC-5000 — на соответствие ТУ /Т Серия /АОЗТ «Защита информации»

60 /82 /26.03.97 /26.03.2000 /ELITE /Программная система ЗИ от НСД в

составе системы управления, обработки, хранения, поиска и передачи электронных документов (шифр ELITE) — по классу 5 для СВТ /П /000 «Компания» «Открытые системы»

61 /83 /26.03.97 /26.03.2000 / /Система гарантированного уничтожения файлов и затирания остаточной информации на магнитных носителях и в памяти ЭВМ (СГУ-1)—по классу 3 для СВТ /П Серия /Гос.унитарн.предпр. «Специализированный центр прогр. систем «Спектр» ГНИИ моделир. и интеллект, сложных систем

62 /84 /21.04.97 /21.04.2000 /«SVINKA-U» /Система защиты информации для ОС UNDO «SVINKA-U» версии 1.20 — по классу 4 для СВТ /П 10 экз. /ЗАО «Релком-Альфа»

63 /85 /10.04.97 /10.04.2000 /- /Защищенная «Мобильная сетевая система управления базами данных «Линтер-ВС» версии 5.1 — по классу защищенности 3 для СВТ /П /ВНИИНС

64 /86 /11.04.97 /11.04.2000 /«AS-101» /Интегрированная система охранной сигнализации и контроля доступа «AS-101»—по классу ЗА для АС /ПТ Серия /АОЗТ «РНТ»

65 /87 /11.04.97 /11.04.2000 /- /Персональные ЭВМ торговой марки «Эврика — ТеЗис» — по нормам эффект, защиты АСУ и СВТ от утечки за счет ПЭМИН—для объектов категории 2 /Т Партия /ЗАО «Эврика» ЗАО «Межотраслевой научно-технический центр «ТеЗис»

Продолжение приложения 8

№ п/п /Регистрационный номер сертификата /Дата внесения в государственный реестр /Срок действия сертификата /Наименование средства (шифр) /Предназначение средства (область применения), краткая характеристика параметров /Тип средства /Заявитель

66 /88 /11.04.97 /11.04.2000 /- /Сетевой адаптер IOLANET и вокодер 4800 изделия «Выстрел» (заводские № с 000196 по 000296 включительно) — на соответствие ТУ /Т 101 экз. /Завод «Электроприбор»

67 /89 /24.04.97 /24.04.2000 /DALLAS LOCK 4.0 /Программно-аппаратный комплекс защиты от НСД и обработки конфиденциальной информации /ПА Серия /Ассоциация защиты информации «Конфидент»

68 /90 /16.05.97 /16.05.2000 /«Аккорд» /Комплекс «Аккорд-1.35» и его модификации /ПА Серия /ОКБ САПР ТОО «Фирма «Информкрипт Лтд.»

69 /91 /24.06.97 /24.06.2000 /«Бета» /Учрежденческо-производственная АТС «Бета»—на соответствие «Норм эффективности защиты технических средств передачи речевой, телеграфной и телекодовой информации от утечки информации за счет ПЭМИН», «Норм эффективности защиты АСУ и ЭВТ от утечки за счет ПЭМИН» — для объектов категории 3, по классу защищенности ЗА для АС /ПА Серия /АООТ «Интелтех» АО «Завод «Красная заря»

70 /92 /26.06.97 /26.06.2000 /«ЗОНА-1» /Комплекс акустической и вибрационной защиты «ЗОНА-1»(партия из 200 экз. № 0001—0200) — на соответствие ТУ — для объектов категории 3 /Т 200 экз. /000«ВЕНАВИТ»

71 /95 /16.05.97 /16.05.2000 /МСВС /Средства защиты информации от НСД операционной системы «Мобильная система вооруженных сил» — по классу 5 для СВТ /П /ВНИИ Автоматизации управления в непромышленной сфере

72 /96 /10.06.97 /10.06.2000 /Optima /Система автоматизации технологических процессов формирования документов и организации документооборота для рота «OPTIMA-WorkFlow-SN» версии 1.6 — по классу 1В /П 30 экз. /ЗАО «Оптима»

73 /97 /10.06.97 /10.06.2000 /«Secret Net NT» /Система разграничения доступа « Secret Net NT» версии 1.0 /ПА 100 экз. /ЗАО «Научно-инженерное предприятие «Информзащита»

74 /98 /10.06.97 /10.06.2000 /TN-MS EC-TN-1 /Автоматизированная система управления «Менеджер элементов системы управления TN-MS EC-TN-1» — по классу 1В для АС /П /ЗАО «Метроком»

Продолжение приложения 8

№ п/п /Регистрационный номер сертификата /Дата внесения в государственный реестр /Срок действия сертификата /Наименование средства (шифр) /Предназначение средства (область применения), краткая характеристика параметров /Тип средства /Заявитель

75 /99 /10.06.97 /10.06.2000 /IMACS EMS VERSION 3.0. /Автоматизированная система управления «Менеджер элементов системы управления IMACS EMS VERSION 3.0.» — по классу 1 В для АС /П /ЗАО «Метроком»

76 /104 /27.06.97 /27.06.2000 /TAMS /Программное средство обработки информации «Средство TAMS» — по классу 1Г для АС /П 1экз. /ЗАО «Сеть Глобал Один»

77 /105 /15.07.97 /15.07.2000 /ANG-2000 /Виброакустический шумогенератор ANG-2000 — на соответствие ТУ —для объектов категории 2 /Т Серия /АОЗТ «Защита информации»

78 /106 /23.07.97 /23.07.2000 /«Consono» /30 изделий программно-аппаратного комплекса учрежденческой автоматизированной телефонной станции «Consono» системы MD110 /ПА 30 экз. /ЗАО «ЭРИКССОН КОРПОРАЦИЯ АО»

79 /107 /6.08.97 /6.08.2000 /«Рубеж» /Комплекс средств защиты информации и разграничения доступа к ПЭВМ «Рубеж» — по классу 1Д для АС /ПА Серия /ПО «Старт» НПФ «Кристалл»

80 /108 /21.08.97 /21.08.2000 /«Аккорд Сеть— NetWare4» /Партия (сер. № 0001 — 0100) комплексов средств защиты информации от НСД по классу 1 В для АС и по классу защищенности 3 для СВТ, функционирующих в операционных системах NetWare 4.1, NetWare 4.11 и IntranetWare /ПТ 100 экз. /ОКБ САПР ТОО «Фирма» Информкрипт Лтд»

81 /109 /19.09.97 /19.09.2000 /МП-1А /Устройство защиты телефонных аппаратов на линиях с аналоговой информацией /Т Серия /ТОО «Реном»

82 /110 /19.09.97 /19.09.2000 /МП—1Ц /Устройство защиты телефонных аппаратов на линиях с цифровой информацией /Т Серия /ТОО «Реном»

83 /111 /8.10.97 /8.10.2000 /FireWall-1 /Партия средств программного обеспечения межсетевого экрана FireWall-1 (серийные № с UNIFW 1.1 по UNIFW 1.5 включительно) — по классу 4 для межсетевых экранов /П 5 экз. /000 «Московская информационная сеть»

84 /112 /22.09.97 /22.09.2000 /«Сатурн» /Система защиты информации от НСД по классу защищенности 3 для СВТ, функционирующая в среде MS Windows 95 на автономных ПЭВМ, на рабочих станциях ЛВС Microsoft Windows и ЛВС Novell NetWare v.3.11—4.1 /П /РЦ «Безопасность»

Продолжение приложения 8

№ п/п /Регистрационный номер сертификата /Дата внесения в государственный реестр /Срок действия сертификата /Наименование средства (шифр) /Предназначение средства (область применения), краткая характеристика параметров /Тип средства /Заявитель

85 /113 /22.09.97 /22.9.2000 /«Микро» v.6 /Средство контроля защищенности информации для ПЭВМ и ЛВС, функционирующее в среде ОС MS DOS (v.3.0 — 6.22), PC DOS (v.3.30 — 6.30), Novell NetWare (v.2.15 — 4.1) и Windows 95 (в режиме эмуляции DOS). Средство стирания остаточной информации на магнитных дисках /П /РЦ «Безопасность»

86 /114 /16.10.97 /16.10.2000 /«FAVORIT E-Z» /Персональные ЭВМ типа PC/AT P-54 (P-55) (торговая марка «FAVOR1TE-Z») /ПА Серия /ЗАО «Ниеншанц-Защита»

87 /115 /8.10.97 /8.10.2000 / /Комплекс защиты информации от несанкционированного доступа «Data Guard/24S» — по классу 5 для межсетевых экранов /ПТ 100 экз. /ЗАО «Сигнал-Ком»

88 /119 /14.10.97 /14.10.2000 /МСВС1.5 /Операционная система МСВС 1.5 — по классу 3 для СВТ и классу 1 В для АСУ /П /ВНИИ Автоматизации управления в непромышленной сфере

89 /120 /14.10.97 /14.10.2000 /МСВС 2.0 /Операционная система МСВС 2.0 — по 2 классу для СВТ и классу 1Б —для АСУ /П /Тоже

90 /121 /14.10.97 /14.10.2000 /«Линтер-ВС» /Система управления базами данных «Линтер-ВС» — по классу 2 для СВТ и классу 1 А, 2А, 3А—для АСУ /П /« «

91 /122 /28.10.97 /28.10.2000 /«Набат» /Система оперативно-диспетчерской связи с функциями АТС «Набат» /ПА 150 экз. /АО «Лотес»

92 /123 /21.10.97 /14.10.2000 /«Линтер-версия 5» /Система управления базами данных «Линтер-версия 5» /П /ЗАО«НПП «РЕЛЭКС»

93 /124 /26.11.97 /26.11.2000 /«MS REX 400» /Программный комплекс «Электронный почтамт MS REX 400» версии 4.70.00 /П 1 экз. /ЗАО «Клуб-400»

94 /125 /5.11.97 /5.11.2000 /«ФОН-В» /Мобильная система виброакустического зашумления «ФОН-В»—для объектов категории 2 /Т Серия /ТОО «Маском»

95 /126 /5.11.97 /5.11.2000 /«VNG-006DM» /Система виброакустического зашумления «VNG-006DM» — для объектов категории 2 /Т Серия /ТОО «Маском»

Продолжение приложения 8

№ п/п /Регистрационный номер сертификата /Дата внесения в государственный реестр /Срок действия сертификата /Наименование средства (шифр) /Предназначение средства (область применения), краткая характеристика параметров /Тип средства /Заявитель

96 /127 /5.11.97 /5.11.2000 /«Холст -Л» /Изделие «Холст-Л» (включает СУБД «Линтер-ВС» версии 5, ОС МСВС версии 2.0) — по классу 2 для СВТ /П /ВНИИНС

97 /128 /5.11.97 /5.11.2000 /«Холст -Б» /Базовый программно-технический комплекс «Холст-Б» (включает ОС МСВС версии 2.0, функционирует на ЭВМ «Багет» РС-486-DX2/66) — по классу 2 для СВТ /ПА Серия /ВНИИНС

98 /129 /5.11.97 /5.11.2000 /«Холст» /Типовой программно-технический комплекс «Холст» (включает СУБД «Линтер-ВС» версии 5, ОС МСВС версии 2.0, функционирует на ЭВМ «Багет» РС-4t86-DX2/66) — по классу 2 для СВТ /ПА Серия /ВНИИНС

99 /- 130 /5.11.97 /5.11.2000 /«Холст -С» /Типовой защищенный программно-технический комплекс «Холст-С» (включает СУБД «Линтер-ВС» версии 5, ОС МСВС версии 2.0, функционирует на ЭВМ «Багет» РС-486-DX2/66, реализует функции сервера локальной сети) — по классу 2 для СВТ /ПА Серия /ВНИИНС

100 /133 /3.12.97 /3.12.2000 /УРНМД /Устройство размагничивания накопителей на жестких магнитных дисках УР НМД — на соответствие ТУ /Т 1 экз. /ГМНТЦ «Наука»

101 /135 /16.12.97 /16.12.2000 /«StopFile» /Подсистема разграничения доступа «StopFile»— по классу 4 для СВТ /ПА Серия /ГНПП «Рубин»

102 /136 /16.12.97 /16.12.2000 /СБИЗ /Система СБИЗ версии 1.0 — по классу 4 для СВТ /П /НИИ Автоматической аппаратуры им В.С.Семенихина

103 /137 /23.12.97 /23.12.2000 / /Персональные ЭВМ типа РС/АТ — для объектов категории 2 . /ПА Партия /Северо-Кавказское управление внутренних дел на транспорте

104 /138 /23.12.97 /23.12.2000 /МСВТ 1.0 /Операционная система МСВТ 1.0 — по классу 5 для СВТ /П /ВНИИНС

105 /139 /23.12.97 /23.12.2000 /«Линтер-ВТ 1.0» /Система управления базами данных «Линтер-ВТ» версии 1.0 — по классу 5 для СВТ /П /ВНИИНС

Продолжение приложения 8

№ п/п /Регистрационный номер сертификата /Дата внесения в государственный реестр /Срок действия сертификата /Наименование средства (шифр) /Предназначение средства (область применения), краткая характеристика параметров /Тип средства /Заявитель

106 /140 /16.12.97 /16.12.2000 /«Definity» /Единичный образец коммуникационной станции «Definity» № 96PD 10967342 (программное обеспечение ver.4), система разграничения доступа к функциям администрирования станции « Definity» — по классу 1В для АСУ /ПА 1 экз. /000 «Компания АйСиЭс»

107 /141 /25.12.97 /25.12.2000 /PTDR018 /Программно-аппаратный комплекс PTDR 018 — на соответствие ТУ /ПА Серия /000 «Смерш Техникс»

108 /142 /5.01.98 /5.01.2001 /«Гранит П-М» /Станция прямой связи «Гранит II-М» для основных технических средств и систем категории 2 /Т Серия /ОАО «Псковский завод АТС»

109 /143 /5.01.98 /5.01.2001 /«Юнинт» /Вычислительный комплекс « Юнинт» — по классу 2 для СВТ /П /ВНИИНС

110 /144 /9.01.98 /9.01.2001 /«Текос» /Защищенная система передачи и обработки информации « Текос» — по классу 1 Б для АСУ /П /ТОО «Компания «Текос Лтд.»

111 /145 /9.01.98 /9.01.2001 /«Застава» /Межсетевой экран «Застава» — по классу 3 для межсетевых экранов /П /ОАО «Элвис+»

112 /146 /14.01.98 /14.01.2001 /«Застава-Джет» /Аппаратно-программный комплекс « Застава-Джет» — по классу 2 для СВТ /ПА 1 экз. /АОЗТ «Инфосистемы Джет»

113 /146/1 /2.06.98 /2.06.2001 /«Застава-Джет» /Партия из 10 экземпляров аппаратно-программного комплекса «Межсетевой экран Застава-Джет» — по классу 2 для МЭ /МЭ 10 экз. /Тоже

114 /147 /14.01.98 /14.01.2001 / /Персональные ЭВМ типа PC/AT — для объектов категории 3 /ПА 6 экз. /Ростовский научно-исследовательский институт радиосвязи

115 /148 /28.01.98 /28.01.2001 /ФСП-1Ф- 7А /Фильтр сетевой помехоподавляющий ФСП-1 Ф-7А — на соответствие ТУ /Т Серия /ЗАО «Приборостроитель»

116 /149 /28.01.98 /28.01.2001 /«Гном-3» /Генератор шума «Гном-3» — на соответствие ТУ /Т Серия /Тоже

117 /150 /4.02.98 /4.02.2001 /«REDWALL» /Система защиты информации от несанкционированного доступа «REDWALL» /ПТ Серия /ТОО «КОМИНФОР»

Продолжение приложения 8

Не п/п /Регистрационный номер сертификата /Дата внесения в государственный реестр /Срок действия сертификата /Наименование средства (шифр) /Предназначение средства (область применения), краткая характеристика параметров /Тип средства /Заявитель

118 /151 /29.01.98 /29.01.2001 /«Россия» /Партия из 100 экземпляров голографических специальных защитных знаков типа «Россия» — по классу 3 для СЗЗ /СЗЗ[1] 100 экз. /ЗАО «НПО «Криптон»

119 /152 /12.02.98 /12.02.2001 / /Партия из 1000 экземпляров программных средств защиты информации от вторжения компьютерных вирусов «AVP Евгения Касперского» — на соответствие ТУ /П 1000 экз., /ЗАО «Барьер-1»

120 /153 /19.02.98 /19.02.2001 /«Аккорд-1.95» /Комплекс «Аккорд-1.95» — по классу 1 В для АС /ПТ Серия /ОКБ САПР ТОО «Фирма» «Информкрипт Лтд.»

121 /154 /21.04.98 /21.04.2001 /«Трап» /Партия из 50 экземпляров изделия «Система измерительная автоматизированная К6-6» (зав. № с 001 по 050) — на соответствие ТУ /Т 50 экз. /ГНПП «Информакустика»

122 /155 /24.02.98 /24.02.2001 /«Застава» /Межсетевой экран «Застава» по классу 3 для МЭ /П /АОЗТ «Элвис+»

123 /156 /24.02.98 /24.02.2001 /«Багет» /Партия из 200 экземпляров ЭВМ «Багет-11-05» и «Багет-11-Об»—для объектов категории 2 и 3, при условии выполнения требований, приведенных в ЮКСУ.466225.002 ТУ /ПА 200 экз. /КБ «Корунд-М»

124 /157 /26.02.98 /26.02.2001 /ЛГШ-101 /Партия из 100 экземпляров генератора шума ЛГШ-101 «Рубеж» (№0131010— 0131109) /Т 100 экз. /АОЗТ «Лаборатория ППШ»

125 /158 /26.02.98 /26.02.2001 /ЛГШ-102 /Партия из 100 экземпляров генератора шума ЛГШ-102 «РаМЗес-Авто» (№ 0140010 — 0140109) /Т 100 экз. /Тоже

126 /159 /26.02.98 /26.02.2001 /ЛГШ-103 /Партия из 100 экземпляров генератора шума ЛГШ-103 «РаМЗес-Дубль» (№ 0150009.— 0150108) /Т 100 экз. /« «

127 /160 /21.04.98 /21.04.2001 /«Мрамор ПТ-101» /Партия из 5 0 экземпляров изделия «Мрамор ПТ-101» ИЦАТ 3.843.001-01 ТУ1 (зав.№с01-001 noOl-050) в качестве ВТСС в выделенных помещениях категории 1/Т 50 экз. /ГНПП «Информакустика»

[1] СЗЗ - специальный защитный знак.

Продолжение приложения 8

№ п/п /Регистрационный помер сертификата /Дата внесения в государственный реестр /Срок действия сертификата /Наименование средства (шифр) /Предназначение средства (область применения), краткая характеристика параметров /Тип средства /Заявитель

128 /161 /21.04.98 /21.04.2001 /«Мрамор ПТ-101» /Партия по 50 экземпляров изделия «Мрамор ПТ-101» ИЦАТ 3.843.001-02 ТУ1 (зав. № с 02-001 по 02-050) в качестве ОТСС в выделенных помещениях категории 2 /Т 50 экз. /ГНПП «Информакустика»

129 /162 /21.04.98 /21.04.2001 /«Мрамор ГШ -101» /Партия из 50 экземпляров изделия «Генераторы шума «Мрамор ГШ-101» ИЦАТ 2.119.001 ТУ (зав. № с 001 по 050) — на соответствие «Норм эффективности защиты тех.средств передачи речевой информации от утечки за счет ПЭМИН» /Т 50 экз. /Тоже

130 /163 /26.02.98 /26.02.2001 /КСЗ-ЗИС ДН /Единичный экземпляр изделия «Комплекс средств защиты информации от несанкционированного доступа, встроенных в программное обеспечение элементов защищенных интегрированных сетей двойного назначения, созданных на базе сетевой технологии ГП НИИ «Масштаб» (КСЗ-ЗИС ДН) — по классу 4 для СВТ и по классу 1 В для АС /П 1 экз. /ГП НИИ «Масштаб»

131 /164 /5.03.98 /5.03.2001 /«Юнинт-П» /Программный комплекс « Юнинт-П» (ПК Юнинт-П») — по классу 2 для СВТ и может быть использован при разработке АС до класса защищенности 1 А включительно /П /ВНИИНС

132 /165 /20.03.98 /20.03.2001 /ТПУ-5 /Телефонное проверочное устройство ТПУ-5 — на соответствие ТУ /Т Серия /000 «Геликор»

133 /166 /26.03.98 /26.03.2001 /«Россия» /Голографический специальный защитный знак типа «Россия» — по классу 3 для СЗЗ /СЗЗ Серия /ЗАО «НПО «Криптон»

134 /167 /26.03.98 /26.03.2001 /«Аккорд-Рубеж» /СЗИ от НСД на изолированном рабочем месте и в ЛВС «Аккорд-Рубеж» версии 1.3 — по

классу 1 Г для АСУ /ПТ Серия /ОКБ САПР ТОО «Фирма «Информкрипт Лтд.»

135 /168 /26.03.9 /26.03.2001 /«Oracle 8 Server» /Встроенные элементы защиты информации единичного экземпляра системы управления базами данных «Oracle 8 Server» версии 8.0.3 (серийный номер А5 5143-01) — по классу 1В для АС /П 1 экз. /Представительство Oracle Nederland B.V.

136 /169 /31.03.98 /31.03.2001 /«Прокруст» /Партия из 50 экземпляров подавителя диктофонных закладок ПТЗ-003 «Прокруст» — на соответствие ТУ (№S/N98/4270-5/98/4319) /Т 50 экз. /ЗАО «НПЦ фирма «Нелк»

Продолжение приложения 8

№ п/п /Регистрационный номер сертификата /Дата внесения в государственный реестр /Срок действия сертификата /Наименование средства (шифр) /Предназначение средства (область применения), краткая характеристика параметров /Тип средства /Заявитель

137 /171 /24.04.98 /24.04.2001 /«Cyber Guard» /Партия из 20 экземпляров межсетевого экрана «Cyber Guard» версии 4.0, (серийные № с 1 -20 по 20-20) — по классу 3 для СВТ /П 20 экз. /ЗАО «Оптима»

138 /173 /17.04.98 /17.04.2001 /«ALTAVISTA FIREWALL 97» /3 единичных образца программного обеспечения межсетевого экрана «ALTAVISTA FIREWALL 97» — по классу 3 для МЭ /П 3 экз. /000 «Анкей» Московское представительство Digital Equipment Corporation

139 /175 /14.04.98 /14.04.2001 /«Bay Networks» /Единичные экземпляры аппаратно-программных комплексов на базе маршрутизаторов «Bay Networks»: Advanced Remote Node—зав. № NEPOO 17306, Access Stack Node 2(ASN2)—зав. № AF0002012, BackBone Node(BN)—зав.№BLA01816 —по классу 4 для МЭ /ПТ 3 экз. /АОЗТ «Инфосистемы Джет»

140 /176 /27.04.98 /27.04.2001 / /Партия из 3 персональных ЭВМ типа PC/AT с установленными в них СЗИ ГШ-К-100 для объектов ЭВТ категории 2 /ПТ 3 экз. /Управление ФСБ РФ по Ставропольскому краю

141 /177 /27.04.98 /27.04.2001 / /Партия из 3 персональных ЭВМ типа PC/AT — для объектов ЭВТ категории 2 /ПТ 3 экз. /Главное управление ЦБ РФ по Ставропольскому краю

142 /178 /29.04.98 /29.04.2001 / /Система защиты информации от несанкционированного доступа «Криптон-Вето 1.0» /ПТ Серия /000 «Фирма «Анкад»

143 /180 /17.06.98 /17.06.2001 /«КТЛ-400» /Партия из 50 экземпляров контроллера телефонной линии «КТЛ-400» — на соответствие ТУ (№05001—05050) /Т 50 экз. /АОЗТ «Защита информации»

144 /181 /2.06.98 /2.06.2001 /DALLAS LOCK 4.1. /Программно-аппаратный комплекс защиты от НСД DALLAS LOCK 4.1 — по классу 3 для СВТ /ПА Серия /Ассоциация защиты информации «Конфидент»

145 /182 /25.05.98 /25.05.2001 / /Партия из 3 персональных ЭВМ типа PC/AT—для объектов категории 3 /ПТ 3 экз. /Ростовский НИИ радиосвязи

Продолжение приложения 8

№ п/п /Регистрационный номер сертификата /Дата внесения в государственный реестр /Срок действия сертификата /Наименование средства (шифр) /Предназначение средства (область применения), краткая характеристика параметров /Тип средства /Заявитель

146 /183 /10.06.98 /10.06.2001 / /Партия из 30 изделий автоматизированной системы разграничения доступа «Пандора» на базе « Gauntlet» версии 3.1.) —по классу 3 для МЭ (№1-30—30-30) /МЭ 30 экз. /АО «Релком-Альфа»

147 /184 /10.06.98' /10.06.2001 / /Партия из 30 изделий «Автоматизированной системы разграничения доступа Black Hole версии BSDI» — по классу 3 для МЭ (№ 1 -30 — 30-30) /МЭ 30 экз. /Тоже

148 /185 /10.06.98 /10.06.2001 / /Комплект программ антивирусной защиты «DSAV 2.51» — на соответствие ТУ /П /ЗАО «ДиалогНаука»

149 /186 /17.06.98 /17.06.2001 /«ДИК» /Система защиты информации «ДИК» по классам 3Б и 2Б—для АС /ПА Серия /ЗАО «Ниеншанц-Защита»

150 /187 /17.06.98 /17.06.2001 /«Туман» /Единичный образец устройства защиты информации «Туман»— на соответствие ТУ /Т 1 экз. /Тоже

151 /189 /16.07.98 /16.07.2001 /«Квант-Е» /Цифровая электронная автоматическая телефонная станция «Квант-Е» — для объектов категории 3 /ПА Серия /ОАО «Московская цифровая телефонная компания» АООТ «Импульс»

152 /190 /16.07.98 /16.07.2001 / /Единичный экземпляр системы защиты информации «FireWall-1» версии 3.Ob (серийный № 71151000305) — по классу 6 для СВТ, по классу 4 для МЭ /П 1 экз. /ЗАО Центральная станция технологической связи РАО «Газпром»

153 /191 /17.07.98 /17.07.2001 /«Аккорд-АМДЗ» /Комплекс «Аккорд-АМДЗ» — по классу 1 Б для АС /ПА Серия /ОКБ САПР ТОО «Фирма «Информкрипт» Лтд»

154 /192 /26.08.98 /26.08.2001 /«Лабиринт» /Система защиты информации на ПЭВМ (шифр «Лабиринт») — по классу 3 для СВТ /ПА /

155 /193 /25.08.98 /25.08.2001 / /Единичный экземпляр средств защиты от несанкционированного доступа к информации, встроенных в программное обеспечение многопротокольного маршрутизатора ТЕЯИ.00026 — по классу 3А для АС /П 1 экз. /ОАО «ИСТ НПП «Радуга»

Продолжение приложения 8

№. п/п /Регистрационный номер сертификата /Дата внесения в государственный реестр /Срок действия сертификата /Наименование средства (шифр) /Предназначение средства (область применения), краткая характеристика параметров /Тип средства /Заявитель

156 /194 /1.09.98 /1.09.2001 / /Межсетевой экран FireWall/Plus for Windows NT— по классу 4 для МЭ (№ FEA30B4792910A02 — FEA30B4792910A33) /П 32 экз. /Ассоциация защиты информации «Конфидент»

157 /195 /2.09.98 /2.09.2001 / /Система анализа защищенности IP-сетей «Internet Security Scanner» версии 5.2—на соответствие ТУ (№ ISS 1-100 — 100-100) /П 100 экз. /ЗАО «Информзащита»

158 /196 /2.09.98 /2.09.2001 / /Система разграничения доступа « Secret Net NT» версии 1.0, «Secret Net» версии 3.0, «Secret Net» версии 3.1—по классу 3 для СВТ /ПА /ЗАО «Научно-инженерное предприятие «Информзащита»

159 /197 /2.09.98 /2.09.2001 / /2 экземпляра межсетевого экрана Cisco PK FireWall — по классу 3 для МЭ (№ 06008720,06008722) /ПА 2 экз. /ЗАО «Анкей/ Холдинг»

160 /198 /22.09.98 /22.09.2001 /«Сертификат Р» /Специальные защитные знаки «Сертификат Р» — по классу 1В для СЗЗ ТУ (№ СЗЗ.ОООООО 1.01 — СЗЗ.ОООО 100.01) /СЗЗ 100 экз. /ЗАО «Спецзнак»

161 /199 /29.09.98 /29.09.2001 /TPRC /Стационарная система обнаружения аппаратов магнитной записи (шифр TPRC) — на соответствие ТУ (№ 0001—0050) /ПА 50 экз. /000 «Инженерно-коммерческий многопрофильный центр-1»

162 /200 /4.11.98 /4.11.2001 /«Застава-Джет-РС» /Программный комплекс «Межсетевой экран «Застава-Джет-РС» /П /АОЗТ «Инфосистемы Джет»

163 /201 /19.11.98 /19.11.2001 / /Пакет программ для организации защищенных частных виртуальных сетей (VPN) на различных каналах связи, в локальных и глобальных сетях общего пользования, сети Internet корпоративной наложенной сети «Инфотекс» — по классу 1В для АС и классу 3 для СВТ /П /ОАО «Информационные технологии коммуникационные системы» (Инфотекс)

164 /202 /20.11.98 /20.11.2001 /«Россия-МИД» /Специальный защитный знак «Россия-МИД» по классу 3 для СЗЗ /СЗЗ Серия /ОАО «Концерн «Российские

защитные технологии»
Продолжение приложения 8
№ п/п /Регистрационный номер сертификата /Дата внесения в государственный реестр /Срок действия сертификата /Наименование средства (шифр) /Предназначение средства (область применения), краткая характеристика параметров /Тип средства /Заявитель
165 /203 /23.11.98 /23.11.2001 /«К-Systems» /Персональные ЭВМ «К-Systems» (рабочие станции в модификациях № 4013-902-46507230-97-2, № 4013-902-46507230-97-3) на соответствие «Норм эффективности защиты АСУ и ЭВТ от утечки информации за счет побочных излучений и наводок» для объектов ЭВТ категории 2 /Т Серия /000 «К-Системс»
166 /204 /23.11.98 /23.11.2001 /«К-Systems» /Персональные ЭВМ « К-Systems» (сервер в модификации № 4013-902-46507230-97-1) на соответствие «Норм эффективности защиты АСУ и ЭВТ от утечки информации за счет побочных излучений и наводок» для объектов ЭВТ категории 2 /Т Серия /Тоже
167 /205 /26.11.98 /26.11.2001 /«Комплекс-2000» /Программно-аппаратный комплекс автоматизированного управления «Комплекс/2000»—по классу 1В для АС /ПТ Серия /ОАО «ТЕРНА»
168 /206 /3.12.98 /3.12.2001 / /Встроенные средства защиты операционных систем MS Windows NT 4.0 Server (Service Pack 3, International Release, English) и MS Windows NT 4.0 Workstation (Service Pack 3, Russian Release), соответствуют «Требованиям по защите от несанкционированного доступа к информации в автоматизированных системах учета и контроля ядерных материалов» по классу 3 защищенности /П /Российский федеральный ядерный центр— ВНИИ экспериментальной физики
169 /207 /7.12.98 /7.12.2001 / /Партия объемных топографических знаков «Сервисное обслуживание, 1999 год» типа «Визуальный контроль»— по классу 15 для СЗЗ (№ 0000001 — 1500000) /СЗЗ 1500000 экз. /ЗАО «Инфокристалл»
170 /208 /7.12.98 /7.12.2001 / /Партия объемных топографических знаков «Государственный реестр, 1999 год» типа «Визуальный контроль» — по классу 15 для СЗЗ (№ 000001 — 500000) /СЗЗ 500000 экз. /То же
Продолжение приложения 8
№ п/п /Регистрационный номер сертификата /Дата внесения в государственный реестр /Срок действия сертификата /Наименование средства (шифр) /Предназначение средства (область применения), краткая характеристика параметров /Тип средства /Заявитель
171 /209 /11.12.98 /11.12.1999 / /Партия генераторов радиошума «Radioveil» — на соответствие РД «Средства активной защиты объектов ЭВТ от утечки информации по побочным электромагнитным излучениям и наводкам. Основные требования» для объектов категорий и 3 (№0001—0050) /Т 50 экз. /ЗАО «Радиус. Технические средства безопасности»
172 /210 /22.12.98 /22.12.2001 / /Единичный экземпляр средств защиты информации системы электронной почты, разработанных ОАО «ИСТ НПП «Радуга» и функционирующих под управлением операционных систем Windows NT 4.0 (серверная часть) и Windows 95/Windows NT 4.0 (клиентская часть) по классу 1В для АС /П 1 экз. /ОАО «Институт сетевых технологий «Научно-производственное предприятие «Радуга» (ИСТ НПП «Радуга»)
173 /211 /22.12.98 /22.12.2001 / /Партия изделий «Rival» (Соперник), предназначенная для обнаружения и подавления в автоматическом режиме устройств съема информации по сети электропитания 220 В, 50 Гц — на соответствие ТУ (№ 00010 —00019,000100 — 000139) /Т 50 экз. /ЗАО «Радиус. Технические средства безопасности»
174 /212 /15.01.99 /15.01.2002 / /Единичный экземпляр системы

управления сетевого уровня DACScan/rrM-2000-NM оборудованием синхронной цифровой иерархии (Host ГО 960388202) — по классу 1Д для АС /П 1экз. /ЗАО «ПетерСтар»

175 /213 /15.01.99 /15.01.2002 / /Единичный экземпляр системы управления оборудованием синхронной цифровой иерархии ГГМ-SC (Host ID 960388202) — по классу 1Д для АС /П 1 экз. /ЗАО «ПетерСтар»

176 /214 /29.12.98 /29.12.2001 / /Фильтр сетевой помехоподавляющий (защитное устройство) ФПСК-10-220-98-УХЛ4 для выделенных помещений категории 1,2,3 — на соответствие ТУ /Т Серия /000 «Научно-производственное предприятие «ЭЖОМ»

177 /215 /29.12.98 /29.12.2001 / /Специальный защитный знак типа «Министерство по налогам и сборам РФ» (СЗЗ типа «МНС РФ») — по классу 3 для СЗЗ /СЗЗ Серия /ОАО «Концерн «Российские защитные технологии»

Продолжение приложения 8

№ п/п /Регистрация опций номер сертификата /Дата внесения в государственный реестр /Срок действия сертификата /Наименование средства (шифр) /Предназначение средства (область применения), краткая характеристика параметров /Тип средства /Заявитель

178 /216 /22.01.99 /22.01.2002 / /Партия радиоприемных устройств AR8000 (№ 046941 — 046990) — на соответствие ТУ /Т 50 экз. /ЗАО «Радиус. Технические средства безопасности»

179 /217 /18.02.99 /18.02.2002 / /Единичный экземпляр программно-аппаратного комплекса «Шлюз для передачи почтовых сообщений между изолированными IP-сетями с использованием протокола X.400 поверх X.25» — по классу 3 для МЭ /ПА /Технический центр Банка России

180 /218 /18.03.99 /18.03.2002 / /Единичный образец системы разграничения доступа к функциям администрирования коммуникационной станции Samsung DCS V 1.3 (серийные номера стативовЕ8481б0041,ЕУ48160035)—поклассу6 для СВТ /Т /Компания «Самсунг Электроникс Ко Лтд»

181 /219 /17.03.99 /17.03.2002 / /Комплекс «Аккорд-АМДЗ» версии 1.1 и его модификации, приведенные в приложении к сертификату, — по классу 1Д для АС /ПТ /ОКБ САПР ТОО «Фирма «Информкрипт Лтд.»

182 /220 /26.02.99 /26.02.2002 / /Встроенные средства защиты системы управления базами данных (СУБД) Microsoft SQL Server 6.5 (Service Pack 4, English) на соответствие РД «Требования по защите от НСД к информации в автоматизированных системах учета и контроля ядерных материалов» — по классу 3 /П /Российский федеральный ядерный центр — ВНИИ экспериментальной физики

183 /221 /23.03.99 /23.03.2002 / /Партия радиоприемных устройств AR3000A (№056693— 056792) /Т 100 экз. /ЗАО «Радиус. Технические средства безопасности»

184 /222 /25.03.99 /25.03.2002 /Cisco FIX Firewall /Межсетевой экран Cisco P1X firewall — по классу 3 для МЭ(№ 18011154) /ПА 1 экз. /ОАО «ТВЭЛ»

185 /223 /25.03.99 /25.03.2002 /«Шорох-1» /«Система постановки виброакустических и акустических помех «Шорох-1» — на соответствие ТУ (№ 1083-001 — 1083-100) /Т 100 экз. /000 «Центр безопасности информации «Маском»

Продолжение приложения 8

№ п/п /Регистрационный номер сертификата /Дата внесения в государственный реестр /Срок действия сертификата /Наименование средства (шифр) /Предназначение средства (область применения), краткая характеристика параметров /Тип средства /Заявитель

186 /224 /25.03.99 /25.03.2002 /«Шорох-2» /Система постановки виброакустических и акустических помех «Шорох-2» — на соответствие ТУ (№ 1084-001 —1084-100) /Т 100 экз. /000 «Центр безопасности информации «Маском»

187 /225 /31.03.99 /31.03.2002 / /Программное обеспечение АТС MERIDIAN-1 версии 23—47 под управлением ОС Thor Operation System—по классу 1Д для АС /П 20 экз. /Аккредитованное представительство «Нозерн Телеком Глобал Корпорейшн»

188 /226 /2.04.99 /2.04.2002 /«СП-100» /Специализированный сетевой процессор «СП-100» — по классу 4 для СВТ (№79565306—79565330) /ПТ 25 экз. /Государственный научный центр России Центральный научно-исследовательский и опытно-конструкторский институт робототехники и технической кибернетики

189 /227. /6.04.99 /6.04.2002 / /Генератор шума «SEL SP-21 В 1 Баррикада» — для объектов категории 2 (№ 210 — 239, 261 — 280) /Т 50 экз. /000 «Сюртель»

190 /229 /12.04.99 /12.04.2002 / /Специальный защитный знак типа «Контрольно-кассовая машина» (СЗЗ типа ККМ) — по классу 9 дла СЗЗ /СЗЗ Серия /ОАО «Концерн «Российские защитные технологии»

191 /230 /16.04.99 /16.04.2002 / /Программный комплекс «Межсетевой экран RreWall-1/VPN-l» версии 4.0, Service Pack 2 — по классу 4 для МЭ(№ 00129935,00129940,00129950, 00130119,00144565,0014469) /П 6 экз. /000 «ТОПС Интегратор Систем»

192 /231 /19.04.99 /19.04.2002 /«СЗИ-С» /Специальный защитный знак типа «Система защиты информации» (СЗЗ типа «СЗИ-С») — по классу 3 для СЗЗ /СЗЗ Серия /ОАО «Концерн «Российские защитные технологии»

Продолжение приложения 8

№ п/п /Регистрационный номер сертификата /Дата внесения в государственный реестр /Срок действия сертификата /Наименование средства (шифр) /Предназначение средства (область применения), краткая характеристика параметров /Тип -средства /Заявитель

193 /232 /19.04.99 /19.04.2002 /«СЗИ-П» /Специальный защитный знак типа «Система защиты информации» (СЗЗ типа «СЗИ-П») — по классу 3 для СЗЗ/СЗЗ Серия /ОАО «Концерн «Российские защитные технологии»

194 /233 /29.04.99 /29.04.2002 /«ФПСУ-IP» /Программно-аппаратный комплекс «ФПСУ- IP» — по классу 3 для МЭ /МЭ /000 «АМИКОН» 000 «Фирма «Информкрипт»

195 /234 /12.05.99 /12.05.2002 / /Встроенные средства защиты СУБД Oracle 7 Server версии 7.3.4.0.0 и Oracle 7 Workgroup Server версии 7.3.4.0.0 на соответствие «Требованиям по защите от несанкционированного доступа к информации в автоматизированных системах учета и контроля ядерных материалов» — по классу 3 /П /Российский федеральный ядерный центр -ВНИИ технической физики

196 /235 /12.05.99 /12.05.2002 / /Генератор шума по электросети «SEL SP-41 /С» (№ 101—150)—для объектов категории 1 /Т 50 экз. /000 «Сюртель»

197 /236 /24.05.99 /24.05.2002 / /Программно-аппаратный комплекс МЭ «WatchGuard» (№ WG 100-001 —WG 100-0020)— по классу 4 для МЭ /МЭ 20 экз. /000 «РЕИНБОУ ТЕКНОЛОДЖИС»

198 /237 /24.05.99 /24.05.2002 / /Аппаратура защиты речевой информации от утечки по виброакустическому каналу «Заслон-2М»— на соответствие ТУ /Т Серия /ГУ НПО «Специальная техника и связь» МВД России

199 /238 /27.05.99 /27.05.2002 / /Система разграничения доступа к функциям администрирования коммуникационной станции Definity G3iV4

(серийный номер 95DR03135410, версия программного обеспечения G3V4i.03.0.048.3) — по классу 6 для СВТ /ПА 1 экз. /ЗАО «Микротест»

200 /239 /9.06.99 /9.06.2002 / /Источники бесперебойного питания Smart UPS APS — на соответствие ТУ /Т 96 экз. /12-е Главное управление МО РФ

201 /240 /9.06.99 /9.06.2002 / /Принтеры HP Laser Jet 6P — для объектов категории 2 /Т 20 экз. /Тоже

Окончание приложения 8

№ п/п /Регистрационный номер сертификата /Дата внесения в государственный реестр /Срок действия сертификата /Наименование средства (шифр) /Предназначение средства (область применения), краткая характеристика параметров /Тип средства /Заявитель

202 /241 /9.06.99 /9.06.2002 / /Проекторы hi Focus Lite Pro 720 Проекторы hi Focus Lite Pro 725 — для объектов категории 2 /Т 19 экз. Т 20 экз. /12-е Главное управление МО РФ

203 /242 /4.06.99 /4.06.2002 / /Система защиты информации « Checkpoint FireWall-1/VPN-1» версии 4.0, Service Pack 3 с идентификационным номером изделия CPFW-EVAL-1-FWZ1-V40—по классу 3 для МЭ /П 20 эк». /ЗАО «Научно-производственное предприятие «Безопасные информационные технологии»

204 /243 /23.06.99 /23.06.2002 / /Система цифрового виброакустического шума 4-канальная SEL SP-51 /А — для выделенных помещений категории 1 /Т 100 экз. /000 «Сюртель»

205 /244 /28.06.99 /28.06.2002 / /Единичный образец программного обеспечения МЭ Alta Vista Firewall 98 (регистрационный номер AVFW98-0002097) — по классу 3 для МЭ /П 1экз. /ЗАО «РНТ»

206 /245 /30.06.99 /30.06.2002 / /Виброакустический комплект ВВ30I— на соответствие технического описания /Т Серия /ЗАО «Полет-Элита»

## ЛИТЕРАТУРА


1. Абалмазов Э. И. Направленные микрофоны: мифы и реальность// Системы безопасности. 1996, август-сентябрь. — С. 98—100.
2. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации //Руководящий документ. Утвержден Председателем Государственной технической комиссии при Президенте Российской Федерации.
3. Агеев А. С. Организация работ по комплексной защите информации//Информатика и вычислительная техника. 1993. №1,2. — С. 71—72, 89.
4. Аксенов Л. Осторожно. Вас подслушивают//Новости разведки и контрразведки. 1995. № 7—8 (40—41). — С. 13.
5. Акустика: Справочник. — М.: Радио и связь, 1989. — 336 с.
6. Альбац Е. Мина замедленного действия. — М.: Русслит, 1992. — 416 с.
7. Андрианов В. И., Соколов А. В. Шпионские штучки-2, или Как сберечь свои секреты. — СПб.: Лань, 1997. — 348 с.
8. Андрианов В. И. и др. Шпионские штучки и устройства для защиты объектов и информации. — СПб.: Лань, 1995.—272 с.
9. АО «Т-Хелпер». Прайс-лист. Октябрь. 1994.
10. Атакующая спецтехника «RV» украинской фирмы «ВЕЧЕ». — Защита информации. № 2. 1994. — С. 62—76.
11. Батраков А. С., Минеев В. В. Прикладная оптика. — МО, 1992. — 518

с.
12. «Благополучная» Германия//Частный сыск. Охрана. Безопасность. 1995. № 6. — С. 29.
13. Большая советская энциклопедия, — М.: Советская энциклопедия, 1974. —Т. 9. С. 433—437; Т. 6. С. 244—245; Т, 17. С. 244.
14. «Большое ухо» КГБ в каждом российском доме//Час Пик. 1993. № 8. С. 2.
15. Брусницин Н. А. Открытость и шпионаж. — М.: Воениздат, 1991. — 56 с.
16. Василевский В. И. Реализация современной концепции построения комплексов обнаружения средств негласного съема конфиденциальной информации в последней разработке НПЦ Фирма «НЕЛК» — универсальной базовой поисковой программе ПиН//Системы безопасности. 1996. № 6. Ноябрь — декабрь. — С. 66—67.
17. Вашу безопасность обеспечит техника фирмы «НОВО»//Каталог фирмы. — 1995
18. Виноградов А. В., Волков В. В. Спецтехника. — М.: Лаборатория LB бизнеса, 1996.—13с.
19. Вовченко В. В., Степанов И. О. «Элинвест» в атаке//Защита информации. 1995. № 3. — С. 76—88.
20. Вудворд Б. Признание шефа разведки: Пер. с англ. — М.: Политиздат, 1990. — 479 с.
21. Гасанов Р. М. Промышленный шпионаж на службе монополий. — М.: Политиздат, 1989. — 267 с.
22. Генератор шума «Гном-3»//Паспорт, 1994. — 8с.
23. Гончаров В. Рождество в Афинах//Новости разведки и контрразведки. 1996. № 1(58).
24. Гражданский кодекс Российской Федерации. — М.: Юридическая литература, 1996.—164с.
25. Гредасов Ф. И. Подразделения в разведке/Под ред. Д. А. Гринкевича. — М.: Воениздат, 1988.—256с.
26. Джамса К. Модернизация компьютера/Пер, с англ. — Минск.: Попурри, 1997.—352с.
27. Дмитриев И.И., Рындина Н.Т., Сахаров И.Н. Критерии выбора межсетевых экранов//Технологии и средства связи. 1999. №4—С.82-86.
28. Закон РФ от 11.03.92 г. № 2487—1 «О частной детективной и охранной деятельности »//Российская газета. 1992. № 100. 30 апреля.
29. Закон РФ «О безопасности» (в редакции от 05.03.92 г.).
30. Закон РФ «О правовой охране программ для электронных вычислительных машин и баз данных».
31. Закон РФ «О связи» (в редакции от 20 .01.95 г.).
32. Закон РФ «Об актах гражданского состояния» (в редакции от 15.11.97 г.).
33. Закон РФ «О сертификации продукции и услуг» (в редакции от 10.06.93 г.).
34. Закон РФ № 24—ФЗ от 20.02.95 г. «Об информации, информатизации и защите информации».
35. Закон РФ № 5485—1 от 21.07.93 г. «О государственной тайне».
36. Закон РФ № 4524—1 от 19.02.93 г. «О федеральных органах правительственной связи и информации».
37. Закон РФ «Об оперативно-розыскной деятельности»//Собрание законодательства Российской Федерации. 1995. № 33.
38. Замятин Л. В. Секреты секретных служб//Новости разведки и контрразведки. 1996. № 8 (65) — С. 5.
39. Зотов-Кондратов Э. С. «Альфа-4»: комплект аппаратуры беспроводного видео-наблюдения//Системы безопасности. 1996. № 6(12). Ноябрь — декабрь. — С. 82—83.

40. Измерения в промышленности: Справ, изд. в 3-х кн. Способы измерения и аппаратура: Пер. с нем./Под ред. П. Профоса. — 2-е изд., перераб. и доп. — М.: Металлургия, 1990. — 344 с.
41. Измеритель неоднородности линш1Р5-11//Техническое описание и инструкция по эксплуатации, 1987. - 123 с.
42. Инженерный диплом Шерлока Холмса. — М.: Знание, 1991. — 64 с.
43. Иностранная печать о техническом оснащении полиции зарубежных государств//Информационный бюллетень ВИНИТИ. 1998. № 2. — 44 с.
44. Иоффе В. К., Корольков В. Г., Сапожков М. А. Справочник по акустике/Под ред. М. А. Сапожкова. — М.: Связь, 1979. — 312 с.
45- Калинин А. И., Черенкова Е. Л. Распространение радиоволн и работа радиолиний. — М.: Связь, 1972. — 439 с.
46. Карпов В. В. Маршал Жуков. Опала. Литературная мозаика. — М.: Вече, 1994.—416с.
47. Каталог 1999//НПЦ «Фирма НЕЛК», 1999. — 89 с.
48. Каталог 1995// НПО «Защита информации», 1995. — 56 с.
49. Каталог 1996—1997//НПО «Защита информации», 1997. — 32 с.
50. Каталог наименований сыскной и охранной спецтехники. — НПО «Защита информации», 1994.
51. Каталог технических средств//Фирма «Инко», 1993. — 8с.
52. Кащеев В. И. Цифровой адаптивный фильтр АФ-512//Системы безопасности. 1995. № 1.—С. 51—52.
53. Кейт Х. Мелтон. Шпионские фотокамеры//Безопасность. 1998. № 5. — С.28—31.
54. Киселев А. Е. и др. Коммерческая безопасность/Под ред. В. М. Чаплыгина. — М.: ИнфоАрт, 1993. — 128 с.
55. Ковалев А. Н. Защита информации: правила и механизм лицензирования//Системы безопасности. 1995. № 5. — С. 8—10.
56. Кодекс РСФСР об административных правонарушениях. — М.: Теис, 1996. — 190с.
57. Коммерсантъ-Daily. 1995. № 92. 20 мая.
58. Комплекс конденсаторного микрофона унифицированой серии КМС19—09.
59. Комплекс конденсаторного микрофона унифицированой серии КМС19—05.
60. Комплексные системы защиты информации//Каталог фирмы Дивекон, 1995. — 72 с.
61. Конституция Российской Федерации. —М.: Юридическая литература, 1993. —64с.
62. Контроль людей и их ручной клади на наличие диверсионно-террористических средств//Специальная техника. 1998. № 3. — С. 41—49.
63. Кто прослушивал главу администрации Воронежской области//Сегодня. 1995. № 120. 30 июня 1995.
64. Куренков Е. В., Лысое А. В., Остапенко А. Н. Еще об Истории. О «восьмиэтажном микрофоне»//Конфидент. 1998. № 1. —С. 72—73.
65. Курепков Е. В., Лысов А. В., Остапенко А. Н. Рекомендации по оценке защищенности конфиденциальной информации от ее утечки за счет ПЭМИ//Конфидент. 1998.Мй4.—С.48—50.
66. ЛГШ-101 («Рубеж-01»). Техническое описание и инструкция по эксплуатации// Лаборатория ППШ, 1996. — 8 с.
67. Лихарев С. Б., Фомин Г. А. Обзор средств криптографической защиты информации в персональных компьютерах//Технологии электронных коммуникаций, Т. 45, 1993.—С. 5—48.
68. Лопатин В. В. Правовые аспекты информационной безопасности//Системы безопасности связи и телекоммуникаций. 1998. № 21. — С. 8—10.
69. Лысое А. В., Остапенко А. Н. Промышленный шпионаж в России: методы и средства. — СПб.: Лаборатория ППШ, 1994. — 71 с.
70. Лысое А. В., Остапенко А. Н. Телефон и безопасность. — СПб.: Лаборатория ПГПП, 1995.—105с.

71. Максимов Ю. Н. и др. Защита информации в системах и средствах информатизации и связи. — СПб.: ВИКА, 1996.—113 с.
72. Макаров В. Суперкодированная связь//Красная звезда. 1992.
73. Малогабаритный широкодиапазонный монитор ТК-980//Руководство по эксплуатации. —14 с.
74. Малышка Е. В. Запрет или контроле/Системы безопасности. 1995. № 6. — С. 8—9.
75. Мельников В. В. Защита информации в компьютерных системах. — М.: Финансы и статистика; Электронинформ, 1997.—368с.
76. Микрофоны и телефоны /Справочник. — М.: Радио и связь, 1998. — 236 с.
77. Миниатюрные УКВ ЧМ-передатчики серии «Штифт»/Фирма «Анна», 1995.
78. Мироничев С. Н. Коммерческая разведка и контрразведка, или Промышленный шпионаж в России и методы борьбы с ним. — М.: Дружок, 1995. — 223 с.
79. Надеждин В. С. Технические средства защиты от диктофонов и подслушивающих устройств//Защита информации. 1995. Na3. — С. 72—76.
80. Некрасов М. Ю. Прибор защиты информации 05С-5000//Конфидент. 1998. №2.—С. 99—101.
81. Нелинейный радиолокатор «NR-900M»: Техническое описание. Инструкция по эксплуатации.
82. Об утверждении Временного положения о депозитарной деятельности на рынке ценных бумаг Российской Федерации и порядке ее лицензирования. — Постановление Федеральной комиссии по рынку ценных бумаг № 20 от 2.10.96 г. с изменениями и дополнениями от 16.10.97 г.
83. Об утверждении перечня сведений, составляющих конфиденциальную информацию. — Постановление Правления Пенсионного фонда Российской Федерации № 123 от 30.08.96 г.
84. Об утверждении Положения о депозитарной деятельности в Российской Федерации, установлении порядка введения его в действие и области применения. — Постановление Федеральной комиссии по рынку ценных бумаг № 36 от 16.10.97 г.
85. Об утверждении Правил оказания услуг почтовой связи. — Постановление Правительства Российской Федерации № 1239 от 06.09.95 г.
86. Об утверждении Положений о лицензировании деятельности физических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации, и перечня видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе оперативно-розыскной деятельности. — Постановление Правительства Российской Федерации № 770 от 01.07.96 г.
87. Об обеспечении конфиденциальности в работе с налоговыми декларациями. — Письмо Госналогслужбы РФ от 25.04.97 г. № ИЛ-6-24/321.
88. НПО «Защита информации»//Каталог, 1995.—56 с.
89. Оперативная ЗВуК03aimcb//Knowledge Express, Inc.
90. Оружие шпионажа /Под ред. М. В. Данилова. — М.: Империал, 1994. — 240 с.
91. Остронаправленный микрофон (изделие «ШОРОХ»). Техническое описание.
92. Персональное устройство электронной защиты «M-PROTEC-93» //Техническое описание.
93. Пискарев А. С. Практика работы по лицензированию деятельности в области защиты информации по сертификации продукции по требованиям безопасности информации/ Информационная безопасность: Сб. тезисов

докладов Санкт-Петербургского семинара 17—18 мая 1995 г. — СПб.: СПбГУ, 1995. — С. 25—26.
94. Положение о государственном лицензировании в области защиты информации//Утверждено Решением Государственной технической комиссии при Президенте РФ и Федерального агентства правительственной связи и информации при Президенте РФ от 27.04.94 г. № 10.
95. Положение о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны. — Постановление Правительства Российской Федерации № 333 от 15.04.95 г.
96. Положение о порядке изготовления, ввоза в Российскую Федерацию и использование на территории Российской Федерации радиоэлектронных средств (высокочастотных устройств). — Постановление Правительства Российской Федерации № 643 от 05.06.94 г.
97. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Председателем Государственной технической комиссии при Президенте Российской Федерации 25.11.94 г.
98. Правила Государственной регистрации нормативных правовых актов. — Постановление Правительства Российской Федерации № 1009 от 13.06.94 г.
99. Положение о Государственной комиссии по электросвязи при Министерстве связи Российской Федерации. — Постановление Правительства Российской Федерации Ns 330 от 20.05.92 г.
100. Положение о лицензировании деятельности в области связи в Российской Федерации. — Постановление Правительства Российской Федерации № 642 от 05.06.94 г.
101. Положение о службе государственного надзора за связью в Российской Федерации. — Постановление Правительства Российской Федерации № 1156 от 15.11.93 г.
102. Попугаев Ю. Телефонные переговоры: способы защиты//Частный сыск и охрана. 1995. № 3. — С. 78—84.
103. Предпринимательство и безопасность. — М.: Универсум, 1991, — с. 215—216.
104. Прибор для обнаружения записывающих устройств TRD-800//Фирма CCS.
105. Проект Закона РФ «О коммерческой тайне»//Информатика и вычислительная техника. 1994. № 2—3. — с. 105—108.
106. Прытко С. М., Топоровский Л. Н. Нелинейная радиолокация: принцип действия, область применения, приборы и системы //Системы безопасности связи и телекоммуникаций. 1995. № 6. — С. 52—55.
107. Разъяснение о порядке предоставления сведений ограниченного распространения по запросам сторонних организаций. — Инструктивное письмо Государственной налоговой службы Российской Федерации от 11.05.95 г. № ЮБ-6-18/261.
108. СРМ-700 Зонд-монитор: Руководство пользователя. — Research Electronics Inc.1997.-70с.
109. Римский-Корсаков А. В. Электроакустика. — М.: Связь, 1973. — 373 с.
110. Роб. Тидроу. Управление реестром Windows'95. — СПб.: BHV, 1996. — 280с.
111. Ронге М. Разведка и контрразведка.—Киев: Синто, 1993.—239с.
112. Рудд Ч. А., Степанов С. А. Фонтанка, 16: Политический сыск при царях, М.: Мысль, 1983.—432с.
113. Рыбян А. А. Подразделения в ночном бою. — М.: Воениздат, 1984. — 208 с.
114. Рядовые боевики жили на скромную зарплату//Коммерсантъ-Daily. 1995. № 101 2 июня.

115. Сазонов Д. М. Антенны и устройства СВЧ. —М.: Высш. школа, 1988. -— 432 с.
116. Сапожков М. А. Электроакустика: Учебник для вузов. — М.: Связь, 1978.— 272 с.
117. Селективный транзисторный вольтметр STV-401. Техническое описание и инструкция по эксплуатации. — Berlin: VEB Messelektronik, 1984. — 61с.
118. Селективный микровольтметр и прибор для измерения радиопомех FSM-8.5. Техническое описание и инструкция по эксплуатации. — Berlin: VEB Messelektronik, 1985.—68с.
119. Селективный транзисторный вольтметр STV-301. Техническое описание и инструкция по эксплуатации. — Berlin: VEB Messelektronik, 1984. — 59 с.
120. Селективный микровольтметр и прибор для измерения радиопомех FSM-11. Техническое описание и инструкция по эксплуатации. — Berlin: VEB Messelektronik, 1985.—98с.
121. Синилов В. Г., Ковалев М. С. Телевизионные камеры для использования в целях безопасности //Системы безопасности связи и телекоммуникаций. 1998. №21.—С. 24.
122. Слагаемые безопасности. Каталог средств и систем. — М.: АССА, 1995. — 188с.
123. Специальная электроника//АОЗТ «Бэтмэн», 1995. — 10 с.
124. Сребнев В. И. Поисковый радиомониторинг: проблемы, методики, аппаратура// Системы безопасности. 1999. № 24. Январь — февраль. — С. 58—63.
125. Средства защиты конфиденциальной речевой информации от утечки по линиям радио- и проводной связи «Рокада». — НПО «Заря», 1994.
126. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации//Руководящий документ. Утвержден Председателем Государственной технической комиссии при Президенте Российской Федерации 30.03.92 г.
127. Система сертификации средств криптографической защиты информации//Общие положения.
128. Старый знакомый OSCOR//Системы безопасности. 1999. № 24. Январь — февраль. — С.55.
129. Специальная техника для контроля и защиты информации/Компания ГРОТЕК, 1994. — 89 с.
130. Специальная техника. Системы безопасности и защиты. — М: Knowledge Express Inc., 1994.— 30с.
131. Специальная техника защиты и контроля информации//Каталог фирмы Маском,1995.
132. Специальная техника//Каталог фирмы Нелк. — 1995.
133. Справочник по акустике/Иоффе В. К., Корольков В. Г., Сапожков М. А./Под ред. М. А. Сапожкова. — М.: Связь, 1979. — 312 с.
134. Справочник по радиоизмерительным приборам/Под ред. В. С. Насонова. — М.: Сов. радио, 1979. — Т. 3. — 424 с.
135. Справочник радиолюбителя-конструктора. — М.: Энергия, 1977. — 752 с.
136. Средства защиты информации/Каталог фирмы «Конфидент», 1993.
137. Сырков Б. Ю. Перехват паролей при помощи программных закладок, внедряемых в операционные системы//Системы безопасности связи и телекоммуникаций. 1998. №23.—С. 18—21.
138. Таблица нелинейников//Системы безопасности.
139. Техническая защита//Каталог продукции и услуг. — «Конфидент», 1995. — 42 с.
140. Технические средства защиты информации'99. —М.: ЗАО «АННА», 1999.

— 112с.
141. Технические средства разведки/Под ред. В.И. Мухина. — М.: РВСН, 1992. — 394 с.
142. Технические средства охраны, безопасности и сигнализации //Справочник. Вып. 4. — М.: ВИМИ, 1994. — 28 с.
143. Технические средства безопасности//Информационно-коммерческий центр-1. — 1995.
144. Технический шпионаж и борьба с ним. — Минск, 1993. — 25 с.
145. Топоровский Л. Средства нелинейной радиолокации: реальный взгляд //Системы безопасности связи и телекоммуникаций. 1998. № 23. — С. 94—96.
146. Уайз Д. Охота на кротов. — М.: Международные отношения, 1994. — С. 87.
147. Уголовный кодекс Российской Федерации//Кодекс. 1996. № 29 (161). — 65 с.
148. Уголовно-процессуальный кодекс РСФСР. — М.: Юридическая литература, 1990. — 346 с.
149. Указ Президента РФ № 334 от 3.04.95 г. «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставлении услуг в области шифрования информации»//КомпьюТерра. 1995. № 16. 24 апреля.
150. Указ Президента РФ № 188 от 6.03.97 г, «Перечень сведений конфиденциального характера».
151. Указ Президента РФ № 633 от 23.06.95 г. «О первоочередных мерах по реализации Федерального закона «Об органах федеральной службы безопасности».
152. Указ Президента РФ № 212 от 19.02.99 г. «Положение о Государственной технической комиссии при Президенте Российской Федерации».
153. Указ Президента РФ № 21 от 9.01.96 г. «О мерах по упорядочению разработки, производства, реализации приобретения в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы, а также использованию специальных технических средств, предназначенных для негласного получения информации».
154 Указ Президента РФ № 484 от 15.05.97 года «О представлении лицами, замещающими государственные должности Российской Федерации, и лицами, замещающими государственные должности государственной службы и должности в органах местного самоуправления, сведений о доходах и имуществе».
155. Фролов Г. В. Тайны тайнописи. — М.: Инфосервис Экспресс, 1992. — 124 с.
156. Халяпин Д. Б., Ярочкин В. И. Основы защиты информации. — М.: ИПКИР, 1994.—125с.
157. Халяпин Д. Б., Ярочкин В. И. Основы защиты промышленной и коммерческой информации. — М.: ИПКИР, 1994.—70 с.
158. Хорев А. А. Способы и средства защиты информации. — М.: МО РФ, 1998.-316с.
159. Хорев А. А. Малогабаритные панорамные приемники //Специальная техника 1998.№3.—С.23—27.
160. Шебаршин Л. В. Из жизни начальника разведки. — М.: Международные отношения, 1994. — 192 с.
161. Шелков В. А. Кит Мэлтон и его музей «шпионской» техники//Специальная техника. 1998. № 4—5. — С. 54—64.
162. Шиверский А. А. Защита информации: проблемы теории и практики. — М.: Юрист, 1996.—112с.
163. Шумилов А. Ю. Новый оперативно-розыскной закон. — М.: Фирма АВС, 1997.—47с.

164. Частный сыск и охрана. 1993. № 9. — С. 62—63.
165. Эйдлси Ф. За кулисами ЦРУ/Пер, с англ. — М.: Воениздат, 1979. — 464 с.
166. Энциклопедия промышленного шпионажа 1 Катарин Ю.Ф., Куренков Е.В., Лысов А.В., Остапенко А.Н.; Под ред. Куренкова Е.В. — СПб.: Полигон, 1999. — 512 с.
167. Ярочкин В. И. Служба безопасности коммерческого предприятия. — М.: «Ось-89», 1995.—144с.
168. Ярочкин В. И. Предприниматель и безопасность. Часть II. —М.: Экспертное бюро, 1994. — 64 с.
169. Ярочкин В. И. Технические каналы утечки информации. — М.: ИПКИР, 1994. — 106 с.
170. Ярочкин В. И., Халяпин Д. Б. Основы защиты информации. Служба безопасности предприятия — М.: 1993. — 42 с.
171. Яшин Ю. А. Кто владеет информацией, тот владеет миром//Красная звезда. 1993. № 97 (21084) 29 апреля.
172. Audio Intelligence Devices// Product Catalog, 1992. — 399 p.
173. Audio Intelligence Devices/ Catalog. — Florida USA, 1995.
174. Anics firm// Каталог 1994 г. 99. Communication Control System of New York, LTD//Product Catalog, 1992. — 46 p.
175. AM/FM Stereo Radio. Model ANS-55W. Operation Instruction//DAEWOO. — 5p.
176. Anics firm//Каталог 1994 г. — 68 p.
177. AR-3000A//Technical Specifications. 1993. — 26 p.
178. Armada International. — 1990. — V. 14. — № 2. — P. 91.
179. Armada International. — 1990. — V. 14. — № 3. — P. 14—54.
180. Communication Control System jf New York, LTD//Product Catalog, 1992. — 46 p.
181. Combicontrol 8000 Spesial. Owner's Manual /PAN International. — P. 5.
182. Communication Recever//Icom Inc., 1994. — 12 p.
183. Covert Audio Intercept//Surveillance Tecnology Group. — London, 1993. — 32 p.
184. Electronic Welt'93//Conrad Electronic. — P. 346—358.
185. Electronic Welt'93//Conrad Electronic. ~ P. 385—392.
186. Elsy //Инструкция по эксплуатации. — С. 1.
187. Government Suplier of Surveillance Technology//PK Electronic. — Hamburg, 1994. — 268 p.
188. International Defense Review. — 1987. — № 1 — P. 21.
189. International Logistics System./Catalog, 1993. — P. 56.
190. Jane's Defence Weekly. — 1985. — V. 4, № 2. — P. 236.
191. Jane's Defence Weekly. — 1985. — V. 4, № 2. — P. 236.
192. LEA//Product Catalog. — 1992.—84 p.
193. Mebgerate Mebsysteme. Rohde & Schwarz. — Munich, 1992. — 204.
194. Miniport recever EB 100 (20 to 1000 MHz)//Rohde & Schwarz. Munich. FRD. 1990. — P. 1—2.
195. News Week. — 1985. — V. 106. — № 7. — P. 38—39.
196. Neuhiten 91\94 186. Rohde & Schwarz. — Munich, 1992. — 56 p.
197. NOVO (Вашу безопасность обеспечит техника фирмы «НОВО»)//Каталог продукции и услуг. — 1995. — 69 с.
198. Olimpus. Pearlcorder. — Germany, 1992.
199. PK Anti-riot Equipment. — Hamburg, 1993. — 100 p.
200. PK Electronic intemational//Professional general export catalogue. — Hamburg, London, Paris, New York, № 1. — 268 p.
201. PRO-46//Owners Manual. — 46 p.
202. Price List//A03T «Анна-спецтехника», 17 октября 1995 г.
203. Price List//THT Трейдинг Лтд.

204. Smirab Electronics Ш.//Каталог 1994 г. — 90 р.
205. Spectrum. — 1985. — V. 22. — № 7. — P. 30—38.
206. Spy Head Quoter//Product Catalog, 1992. — 56 p.
207. Stabo XR 100. Руководство по эксплуатации. — 26 р.
208. Stereo Radio Cassete Recorder. Model RQ-A160/170. Operation Instruction// Matsushita Electric Industrial Co. — 79 p.
209. Telecommunication Monitoring //PK Electronic. — 1993. — 18 p.
210. User Information for Radiomonitoring. Rohde & Schwarz. — Munich, 1992.-206p.