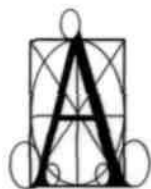


gaudeamus

В. И. Ярочкин

Учебник
для вузов

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ



УДК 002—004
ББК 73—32.97

*Обсуждено отделением Методологии и моделирования
безопасного развития системы процессов» Российской Академии
естественных наук и одобрено к публикации Президиумом РАН*

Рецензенты:

Начальник факультета информационной безопасности ИКСИ
кандидат технических наук **С.Н.Смирнов**

Действительный член Международной академии информатизации
доктор технических наук профессор **А. В. Петраков**

Действительный член Международной академии информатизации
доктор социологических наук профессор **Г. А. Кабакович**

Отв. редактор — кандидат военных наук **Л.И. Филиппенко**

Ярочкин В.И.

Я76

Информационная безопасность: Учебник для студентов
вузов. — М.: Академический Проект; Гаудеамус, 2-е изд.—
2004. — 544 с. (Gaudeamus).

ISBN 5-8291-0408-3 (Академический Проект) ISBN
5-98426-008-5 (Гаудеамус)

В современном информационном обществе информация превратилась в особый ресурс любой деятельности, следовательно, как и всякий другой ресурс, нуждается в защите, в обеспечении ее сохранности, целостности и безопасности. Кто и как угрожает информационной безопасности и как этим угрозам противодействовать, вы узнаете, прочитав эту книгу. Учебник рассчитан на студентов высших учебных заведений, институтов повышения квалификации и школ подготовки специалистов, изучающих проблемы защиты конфиденциальной информации.

УДК 002—004 ББК
73—32.97

ISBN 5-8291-0408-3 © Ярочкин В.И., 2003
©Академический Проект, оригинал-
макет, оформление, 2004
ISBN 5-98426-008-5 © Гаудеамус, 2004

Оглавление:

Введение

Глава 1 КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- 1.1. Основные концептуальные положения системы защиты информации
- 1.2. Концептуальная модель информационной безопасности
- 1.3. Угрозы конфиденциальной информации
- 1.4. Действия, приводящие к неправомерному овладению конфиденциальной информацией

Глава 2 НА ПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- 2.1. Правовая защита
- 2.2. Организационная защита
- 2.3. Инженерно-техническая защита
 - 2.3.1. Общие положения
 - 2.3.2. Физические средства защиты
 - 2.3.3. Аппаратные средства защиты
 - 2.3.4. Программные средства защиты
 - 2.3.5. Криптографические средства защиты

Глава 3 СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ

- 3.1. Общие положения
- 3.2. Характеристика защитных действий

Глава 4 ПРЕСЕЧЕНИЕ РАЗГЛАШЕНИЯ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

- 4.1. Общие положения
- 4.2. Способы пресечения разглашения

Глава 5 ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

- 5.1. Общие положения
- 5.2. Защита информации от утечки по визуальным оптическим каналам
 - 5.2.1. Общие положения
 - 5.2.2. Средства и способы защиты
- 5.3. Защита информации от утечки по акустическим каналам
 - 5.3.1. Общие положения
 - 5.3.2. Способы и средства защиты

- 5.4. Защита информации от утечки по электромагнитным каналам
 - 5.4.1. Защита от утечки за счет микрофонного эффекта
 - 5.4.2. Защита от утечки за счет электромагнитного излучения
 - 5.4.3. Защита от утечки за счет паразитной генерации
 - 5.4.4. Защита от утечки по цепям питания
 - 5.4.5. Защита от утечки по цепям заземления
 - 5.4.6. Защита от утечки за счет взаимного влияния проводов и линий связи
 - 5.4.7. Защита от утечки за счет высокочастотного наводнения
 - 5.4.8. Защита от утечки в волоконно-оптических линиях и системах связи
- 5.5. Защита информации от утечки по материально-вещественным каналам

Глава 6 ПРОТИВОДЕЙСТВИЕ НЕСАНКЦИОНИРОВАННОМУ ДОСТУПУ К ИСТОЧНИКАМ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

- 6.1. Способы несанкционированного доступа
- 6.2. Технические средства несанкционированного доступа к информации
- 6.3. Защита от наблюдения и фотографирования
- 6.4. Защита от подслушивания
 - 6.4.1. Противодействие подслушиванию посредством микрофонных систем
 - 6.4.2. Противодействие радиосистемам акустического подслушивания
 - 6.4.3. Обеспечение безопасности телефонных переговоров
 - 6.4.4. Противодействие лазерному подслушиванию
- 6.5. Противодействие незаконному подключению к линиям связи
 - 6.5.1. Противодействие контактному подключению
 - 6.5.2. Противодействие бесконтактному подключению
- 6.6. Защита от перехвата

Глава 7. КОНФИДЕНЦИАЛЬНОСТЬ ПРИ РАБОТЕ С ЗАРУБЕЖНЫМИ ПАРТНЕРАМИ

- 7.1. Направления взаимодействия с зарубежными партнерами
 - 7.1.1. Научно-техническое сотрудничество с зарубежными партнерами
 - 7.1.2. Научно-техническое сотрудничество. Технологически и обмен и его регулирование.

- 7.1.3. Виды коммерческих международных операций
- 7.1.4. Научно-техническая документация - источник конфиденциальной информации
- 7.1.5. Возможные условия разглашения сведений, составляющих коммерческую тайну
- 7.1.6. Экспертиза ценности передаваемой научно-технической документации
- 7.2. Организация работы с зарубежными партнерами
 - 7.2.1. Оценка потенциальных партнеров
 - 7.2.2. Прием иностранных представителей и проведение коммерческих переговоров
 - 7.2.3. Порядок работы с зарубежными партнерами
 - 7.2.4. Порядок защиты конфиденциальной информации при работе с зарубежными партнерами

Глава 8 АДУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ [^]

Послесловие

Приложения

1. Гостехкомиссия России. Руководящий документ Защита от несанкционированного Доступа к информации. Термины и Определения
2. Доктрина информационной безопасности Российской Федерации
3. Перечень сведений, отнесенных к государственной тайне. Указ президента российской федерации о перечне сведений, отнесенных к государственной тайне. 24 января 1998 года № 61
4. Указ президента российской федерации. Об утверждении перечня сведений конфиденциального характера
5. Положение о лицензировании деятельности по технической защите конфиденциальной информации. Постановление Правительства Российской Федерации от 30 апреля 2002 г. № 290 г. Москва
6. ИНСТРУКЦИЯ по защите конфиденциальной информации при работе с зарубежными партнерами
7. ОБЕСПЕЧЕНИЕ СОХРАНЕНИЯ КОММЕРЧЕСКОЙ ТАЙНЫ ПРЕДПРИЯТИЯ
8. КАТАЛОГ обобщенных мероприятий по защите конфиденциальной информации

Список литературы

Введение [^]

Примечательная особенность нынешнего периода — переход от индустриального общества к информационному, в котором информация становится более важным ресурсом, чем материальные или энергетические ресурсы. Ресурсами, как известно, называют элементы экономического потенциала, которыми располагает общество и которые при необходимости могут быть использованы для достижения конкретных целей хозяйственной деятельности. Давно стали привычными и общепотребительными такие категории, как материальные, финансовые, трудовые, природные ресурсы, которые вовлекаются в хозяйственный оборот, и их назначение понятно каждому. Но вот появилось понятие «информационные ресурсы», и хотя оно узаконено, но осознано пока еще недостаточно. В приводимой литературе так излагается это понятие: «Информационные ресурсы — отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах)». Информационные ресурсы являются собственностью, находятся в ведении соответствующих органов и организаций, подлежат учету и защите, так как информацию можно использовать не только для производства товаров и услуг, но и превратить ее в наличность, продав кому-нибудь, или, что еще хуже, уничтожить.

Собственная информация для производителя представляет значительную ценность, так как нередко получение (создание) такой информации — весьма трудоемкий и дорогостоящий процесс. Очевидно, что ценность информации (реальная или потенциальная) определяется в первую очередь приносимыми доходами.

Особое место отводится информационным ресурсам в условиях рыночной экономики.

Важнейшим фактором рыночной экономики выступает конкуренция. Побеждает тот, кто лучше, качественнее, дешевле и оперативнее (время — деньги!) производит и продает. В сущности, это универсальное правило рынка. И в этих условиях основным выступает правило: кто владеет информацией, тот владеет миром.

В конкурентной борьбе широко распространены разнообразные действия, направленные на получение (добывание, приобретение) конфиденциальной информации самыми

различными способами, вплоть до прямого промышленного шпионажа с использованием современных технических средств разведки. Установлено, что 47% охраняемых сведений добывается с помощью технических средств промышленного шпионажа.

В этих условиях защите информации от неправомерного овладения ею отводится весьма значительное место. При этом «целями защиты информации являются: предотвращение разглашения, утечки и несанкционированного доступа к охраняемым сведениям; предотвращение противоправных 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, имеющих 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».

Как видно из этого определения целей защиты, *информационная безопасность* — довольно емкая и многогранная проблема, охватывающая не только определение необходимости защиты информации, но и то, как ее защищать, от чего защищать, когда защищать, чем защищать и какой должна быть эта защита.

Основное внимание автор уделил защите конфиденциальной информации, с которой большей частью и встречаются предприниматели негосударственного сектора экономики.

Автор вполне осознает и отдает себе отчет в сложности проблемы защиты информации вообще, и с помощью технических средств в частности. Тем не менее свой взгляд на эту проблему он излагает в этой книге, считая, что этим он охватывает не все аспекты сложной проблемы, а лишь определенные ее части.

* * *

Грядущий XXI век будет веком торжества теории и практики информации — информационным веком.

Глава 1 КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ [^]

Что храним, то и имеем

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ - это состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государств».
(Закон РФ «Об участии в международном информационном обмене»)

Постулаты

1. Информация — это всеобщее свойство материи.
2. Любое взаимодействие в природе и обществе основано на информации.
3. Всякий процесс совершения работы есть процесс информационного взаимодействия.
4. Информация—продукт отражения действительности.
5. Действительность отражается в пространстве и времени.
6. Ничего не происходит из ничего.
7. Информация сохраняет свое значение в неизменном виде до тех пор, пока остается в неизменном виде носитель информации — ПАМЯТЬ.
8. Ничто не исчезает просто так.

Понятие «информация» сегодня употребляется весьма широко и разносторонне. Трудно найти такую область знаний, где бы оно не использовалось. Огромные информационные потоки буквально захлестывают людей. Объем научных знаний, например, по оценке специалистов, удваивается каждые пять лет. Такое положение приводит к заключению, что XXI век будет веком торжества теории и практики ИНФОРМАЦИИ — информационным веком.

Правоммерно задать вопрос: что же такое информация? В литературе дается такое определение: информация — сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. Известно, что информация может иметь различную форму, включая данные, заложенные в

компьютерах, «синьки», кальки, письма или памятные записки, досье, формулы, чертежи, диаграммы, модели продукции и прототипы, диссертации, судебные документы и другое.

Как и всякий продукт, информация имеет потребителей, нуждающихся в ней, и потому обладает определенными потребительскими качествами, а также имеет и своих обладателей или производителей.

С точки зрения потребителя, качество используемой информации позволяет получать дополнительный экономический или моральный эффект.

С точки зрения обладателя — сохранение в тайне коммерчески важной информации позволяет успешно конкурировать на рынке производства и сбыта товаров и услуг. Это, естественно, требует определенных действий, направленных на защиту конфиденциальной информации.

Понимая под безопасностью состояние защищенности жизненно важных интересов личности, предприятия, государства от внутренних и внешних угроз, можно выделить и компоненты безопасности — такие, как персонал, материальные и финансовые средства и информацию.

1.1. Основные концептуальные положения системы защиты информации [^]

Анализ состояния дел в сфере защиты информации показывает, что уже сложилась вполне сформировавшаяся концепция и структура защиты, основу которой составляют:

- весьма развитый арсенал технических средств защиты информации, производимых на промышленной основе;
- значительное число фирм, специализирующихся на решении вопросов защиты информации;
- достаточно четко очерченная система взглядов на эту проблему;
- наличие значительного практического опыта и другое.

И тем не менее, как свидетельствует отечественная и зарубежная печать, злоумышленные действия над информацией не только не уменьшаются, но и имеют достаточно устойчивую тенденцию к росту.

Опыт показывает, что для борьбы с этой тенденцией необходима стройная и целенаправленная организация процесса защиты информационных ресурсов. Причем в этом должны

активно участвовать профессиональные специалисты, администрация, сотрудники и пользователи, что и определяет повышенную значимость организационной стороны вопроса.

Опыт также показывает, что:

- обеспечение безопасности информации не может быть одноразовым актом. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных методов, способов и путей совершенствования и развития системы защиты, непрерывном контроле ее состояния, выявлении ее узких и слабых мест и противоправных действий;
- безопасность информации может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты во всех структурных элементах производственной системы и на всех этапах технологического цикла обработки информации. Наибольший эффект достигается тогда, когда все используемые средства, методы и меры объединяются в единый целостный механизм — систему защиты информации (СЗИ). При этом функционирование системы должно контролироваться, обновляться и дополняться в зависимости от изменения внешних и внутренних условий;
- никакая СЗИ не может обеспечить требуемого уровня безопасности информации без надлежащей подготовки пользователей и соблюдения ими всех установленных правил, направленных на ее защиту (рис. 1).



Рис. 1

С учетом накопленного опыта можно определить систему защиты информации как организованную совокупность специальных органов, средств, методов и мероприятий, обеспечивающих защиту информации от внутренних и внешних угроз.

С позиций системного подхода к защите информации предъявляются определенные требования. Защита информации должна быть:

- **непрерывной.** Это требование проистекает из того, что злоумышленники только и ищут возможность, как бы обойти защиту интересующей их информации;
- **плановой.** Планирование осуществляется путем разработки каждой службой детальных планов защиты информации в сфере ее компетенции с учетом общей цели предприятия (организации);

- **целенаправленной.** Защищается то, что должно защищаться в интересах конкретной цели, а не все подряд;
- **конкретной.** защите подлежат конкретные данные, объективно подлежащие охране, утрата которых может причинить организации определенный ущерб;
- **активной.** Защищать информацию необходимо с достаточной степенью настойчивости;
- **надежной.** Методы и формы защиты должны надежно перекрывать возможные пути неправомерного доступа к охраняемым секретам, независимо от формы их представления, языка выражения и вида физического носителя, на котором они закреплены;
- **универсальной.** Считается, что в зависимости от вида канала утечки или способа несанкционированного доступа его необходимо перекрывать, где бы он ни проявился, разумными и достаточными средствами, независимо от характера, формы и вида информации;
- **комплексной.** Для защиты информации во всем многообразии структурных элементов должны применяться все виды и формы защиты в полном объеме. Недопустимо применять лишь отдельные формы или технические средства. Комплексный характер защиты проистекает из того, что защита — это специфическое явление, представляющее собой сложную систему неразрывно взаимосвязанных и взаимозависимых процессов, каждый из которых в свою очередь имеет множество различных взаимообуславливающих друг друга сторон, свойств, тенденций.

Зарубежный и отечественный опыт показывает, что для обеспечения выполнения столь многогранных требований безопасности система защиты информации должна удовлетворять определенным условиям:

- охватывать весь технологический комплекс информационной деятельности;
- быть разнообразной по используемым средствам, многоуровневой с иерархической последовательностью доступа;
- быть открытой для изменения и дополнения мер обеспечения безопасности информации;
- быть нестандартной, разнообразной. При выборе средств защиты нельзя рассчитывать на неосведомленность

злоумышленников относительно ее возможностей;

- быть простой для технического обслуживания и удобной для эксплуатации пользователями;
- быть надежной. Любые поломки технических средств являются причиной появления неконтролируемых каналов утечки информации;
- быть комплексной, обладать целостностью, означающей, что ни одна ее часть не может быть изъята без ущерба для всей системы.

К системе безопасности информации предъявляются также определенные требования:

- четкость определения полномочий и прав пользователей на доступ к определенным видам информации;
- предоставление пользователю минимальных полномочий, необходимых ему для выполнения порученной работы;
- сведение к минимуму числа общих для нескольких пользователей средств защиты;
- учет случаев и попыток несанкционированного доступа к конфиденциальной информации;
- обеспечение оценки степени конфиденциальной информации;
- обеспечение контроля целостности средств защиты и немедленное реагирование на их выход из строя.

Система защиты информации, как любая система, должна иметь определенные виды собственного обеспечения, опираясь на которые она будет выполнять свою целевую функцию. С учетом этого СЗИ может иметь:

- **правовое обеспечение.** Сюда входят нормативные документы, положения, инструкции, руководства, требования которых являются обязательными в рамках сферы их действия;
- **организационное обеспечение.** Имеется в виду, что реализация защиты информации осуществляется определенными структурными единицами, такими как: служба защиты документов; служба режима, допуска, охраны; служба защиты информации техническими средствами; информационно-аналитическая деятельность и другими;
- **аппаратное обеспечение.** Предполагается широкое использование технических средств как для защиты информации, так и для обеспечения деятельности

собственно СЗИ;

- **информационное обеспечение.** Оно включает в себя сведения, данные, показатели, параметры, лежащие в основе решения задач, обеспечивающих функционирование системы. Сюда могут входить как показатели доступа, учета, хранения, так и системы информационного обеспечения расчетных задач различного характера, связанных с деятельностью службы обеспечения безопасности;
- **программное обеспечение.** К нему относятся различные информационные, учетные, статистические и расчетные программы, обеспечивающие оценку наличия и опасности различных каналов утечки и путей несанкционированного проникновения к источникам конфиденциальной информации;
- **математическое обеспечение.** Предполагает использование математических методов для различных расчетов, связанных с оценкой опасности технических средств злоумышленников, зон и норм необходимой защиты;
- **лингвистическое обеспечение.** Совокупность специальных языковых средств общения специалистов и пользователей в сфере защиты информации;
- **нормативно-методическое обеспечение.** Сюда входят нормы и регламенты деятельности органов, служб, средств, реализующих функции защиты информации, различного рода методики, обеспечивающие деятельность пользователей при выполнении своей работы в условиях жестких требований защиты информации.

Под системой безопасности будем понимать организованную совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающих защиту жизненно важных интересов личности, предприятия и государства от внутренних и внешних угроз (рис. 2).

Как и любая система, система информационной безопасности имеет свои цели, задачи, методы и средства деятельности, которые согласовываются по месту и времени в зависимости от условий.

Удовлетворить современные требования по обеспечению безопасности предприятия и защиты его конфиденциальной информации

может только система безопасности.

1.2. Концептуальная модель информационной безопасности [^]

Понимая информационную безопасность как «состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций», правомерно определить угрозы безопасности информации, источники этих угроз, способы их реализации и цели, а также иные условия и действия, нарушающие безопасность. При этом, естественно, следует рассматривать и меры защиты информации от неправомерных действий, приводящих к нанесению ущерба.

Практика показала, что для анализа такого значительного набора источников, объектов и действий целесообразно использовать методы моделирования, при которых формируется как бы «заместитель» реальных ситуаций. При этом следует учитывать, что модель не копирует оригинал, она проще. Модель должна быть достаточно общей, чтобы описывать реальные действия с учетом их сложности.

Можно предложить компоненты модели информационной безопасности на первом уровне декомпозиции. По нашему мнению, такими компонентами концептуальной модели безопасности информации могут быть следующие:

- объекты угроз;
- угрозы;
- источники угроз;
- цели угроз со стороны злоумышленников;
- источники информации;
- способы неправомерного овладения конфиденциальной информацией (способы доступа);
- направления защиты информации;
- способы защиты информации;
- средства защиты информации.

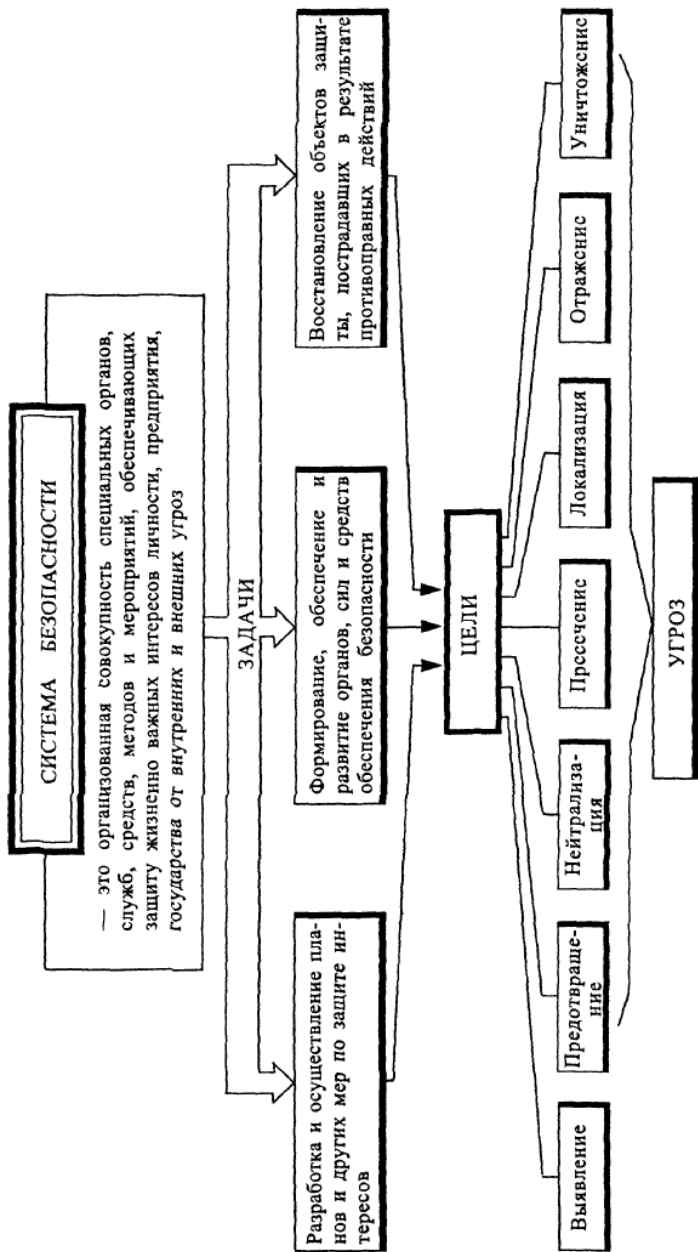


Рис. 2

Объектом угроз информационной безопасности выступают сведения о составе, состоянии и деятельности объекта защиты (персонала, материальных и финансовых ценностей, информационных ресурсов).

Угрозы информации выражаются в нарушении ее целостности, конфиденциальности, полноты и доступности.

Источниками угроз выступают конкуренты, преступники, коррупционеры, административно-управленческие органы.

Источники угроз преследуют при этом следующие цели: ознакомление с охраняемыми сведениями, их модификация в корыстных *целях* и уничтожение для нанесения прямого материального ущерба (рис. 3).

Неправомерное овладение конфиденциальной информацией возможно за счет ее разглашения источниками сведений, за счет утечки информации через технические средства и за счет несанкционированного доступа к охраняемым сведениям.

Источниками конфиденциальной информации являются люди, документы, публикации, технические носители информации, технические средства обеспечения производственной и трудовой деятельности, продукция и отходы производства.

Основными направлениями защиты информации являются правовая, организационная и инженерно-техническая защиты информации как выразители комплексного подхода к обеспечению информационной безопасности.

Средствами защиты информации являются физические средства, аппаратные средства, программные средства и криптографические методы. Последние

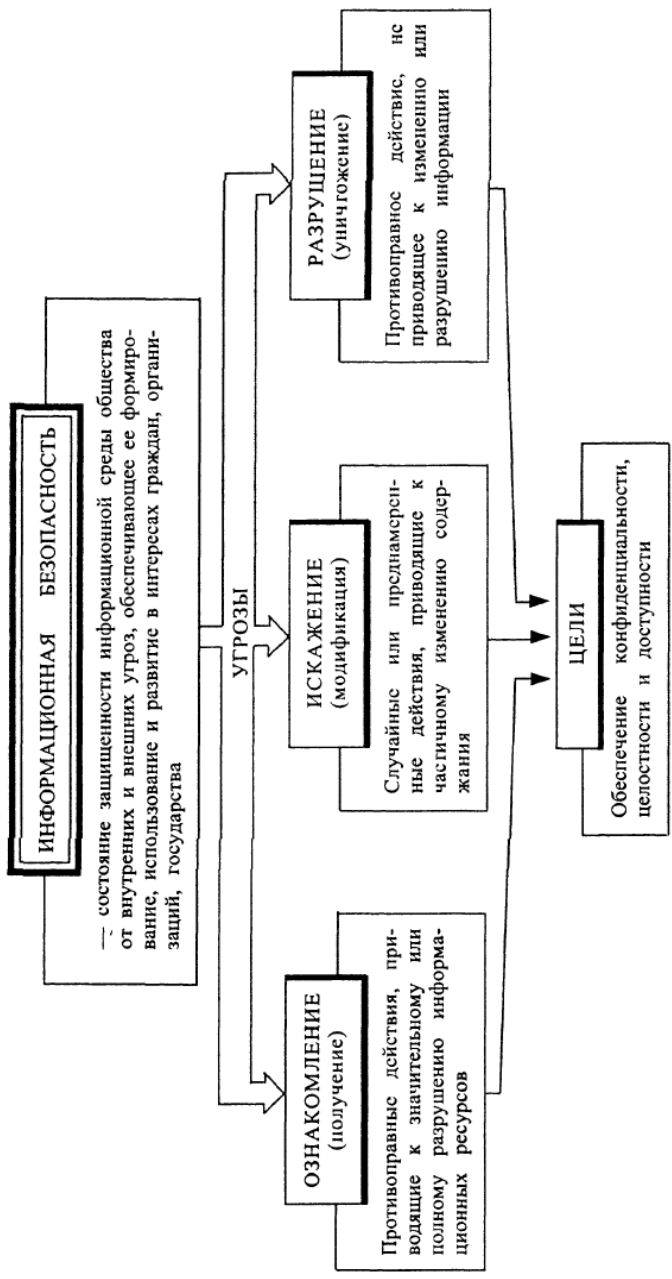


Рис. 3

КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

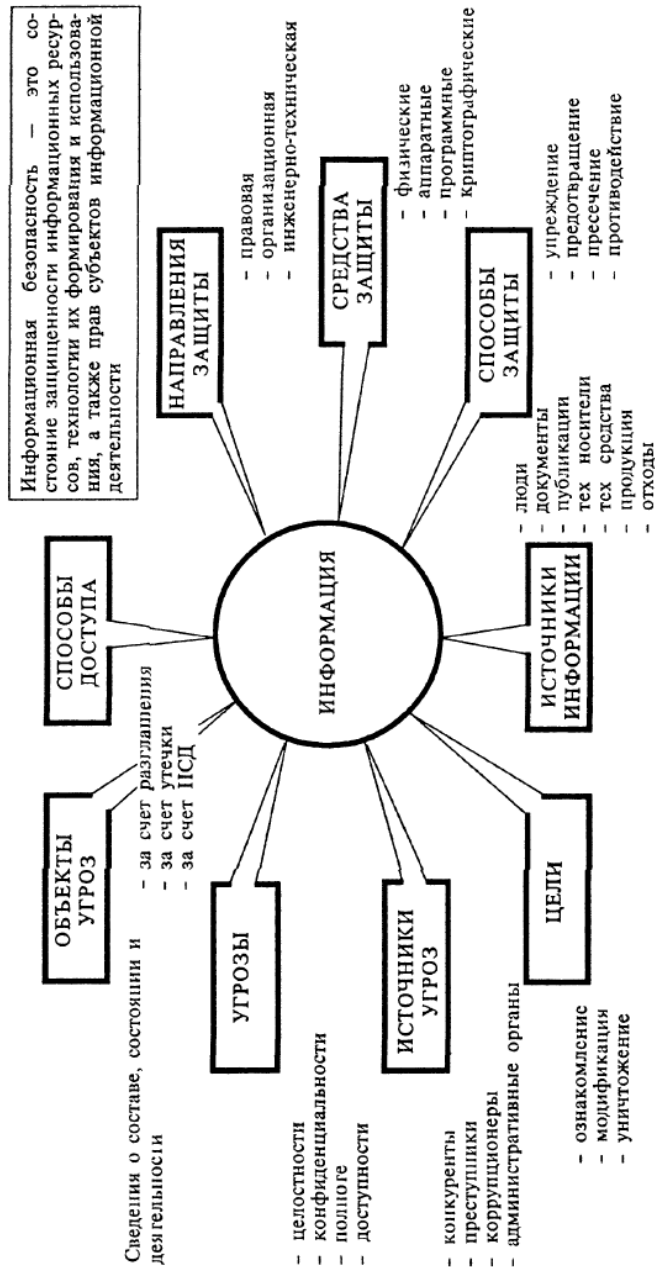


Рис. 4

могут быть реализованы как аппаратно, программно, так и смешанно-программно-аппаратными средствами.

В качестве способов защиты выступают всевозможные меры, пути, способы и действия, обеспечивающие упреждение противоправных действий, их предотвращение, пресечение и противодействие несанкционированному доступу.

В обобщенном виде рассмотренные компоненты в виде концептуальной модели безопасности информации приведены на следующей схеме (рис. 4).

Основные элементы концептуальной модели будут рассмотрены более подробно в следующих разделах книги.

Концепция безопасности является основным правовым документом, определяющим защищенность предприятия от внутренних и внешних угроз.

1.3. Угрозы конфиденциальной информации [^]

Под угрозами конфиденциальной информации принято понимать потенциальные или реально возможные действия по отношению к информационным ресурсам, приводящие к неправомерному овладению охраняемыми сведениями.

Таковыми действиями являются:

- ознакомление с конфиденциальной информацией различными путями и способами без нарушения ее целостности;
- модификация информации в криминальных целях как частичное или значительное изменение состава и содержания сведений;
- разрушение (уничтожение) информации как акт вандализма с целью прямого нанесения материального ущерба.

В конечном итоге противоправные действия с информацией приводят к нарушению ее конфиденциальности, полноты, достоверности и доступности (рис. 5), что в свою очередь приводит к нарушению как режима управления, так и его качества в условиях ложной или неполной информации.

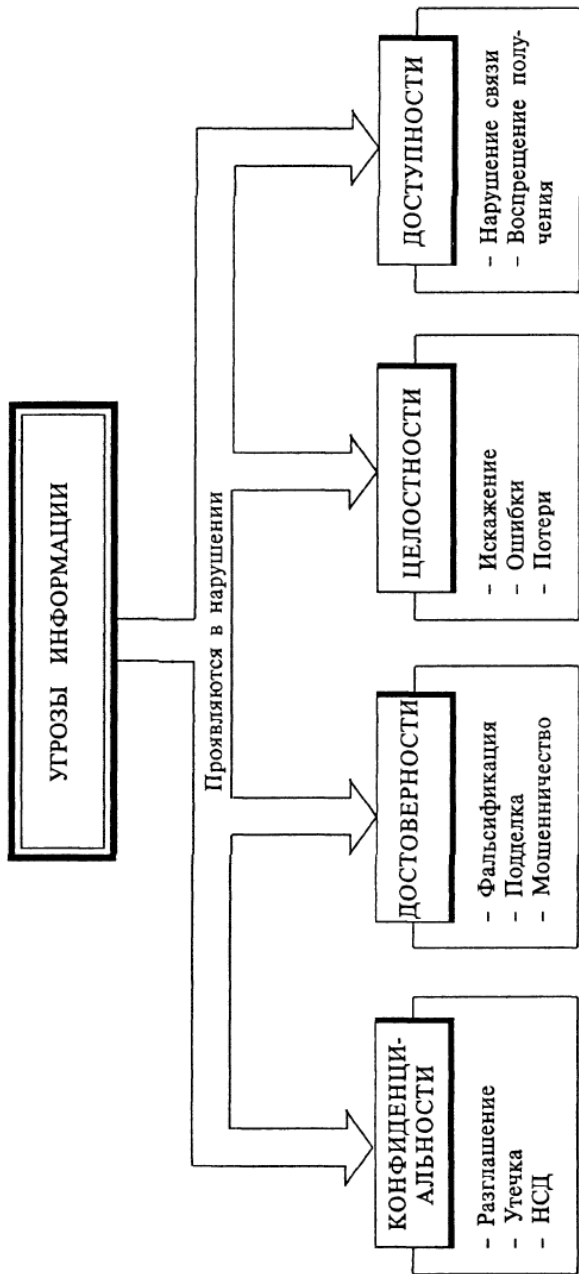


Рис 5

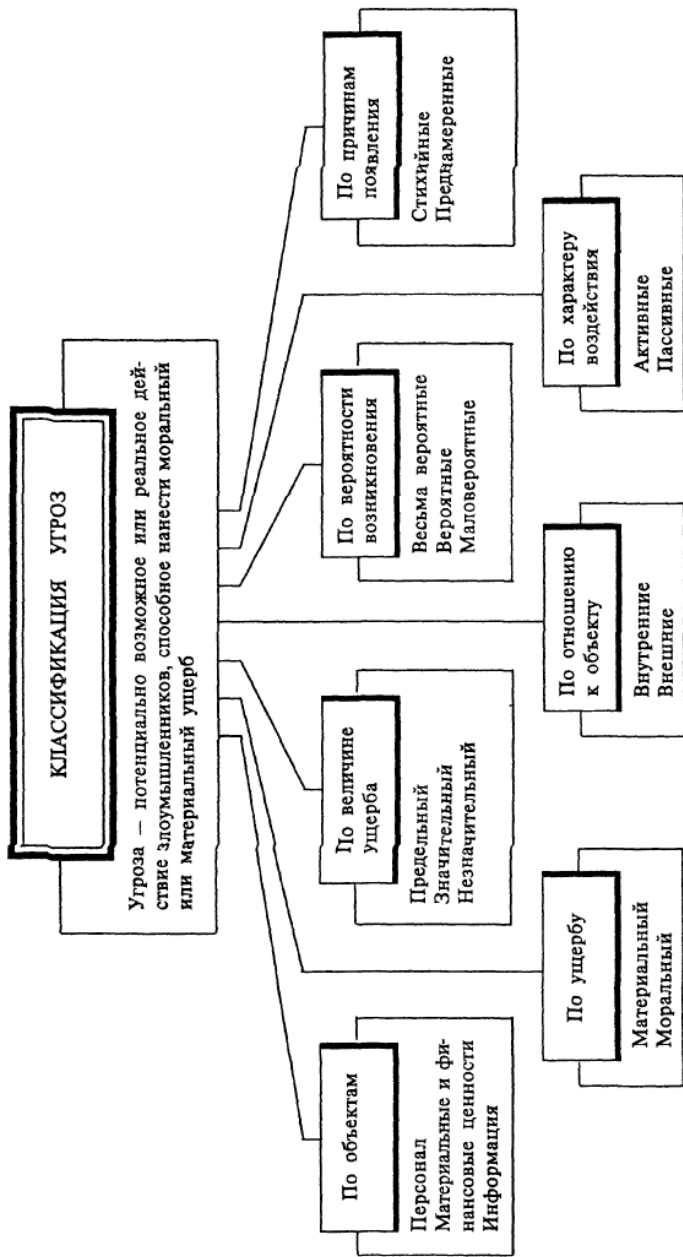


Рис. 6

Каждая угроза влечет за собой определенный ущерб — моральный или материальный, а защита и противодействие угрозе призваны снизить его величину, в идеале — полностью, реально — значительно или хотя бы частично. Но и это удастся далеко не всегда.

С учетом этого угрозы могут быть классифицированы по следующим кластерам, (рис. 6):

—по величине принесенного ущерба:

- предельный, после которого фирма может стать банкротом;
- значительный, но не приводящий к банкротству;
- незначительный, который фирма за какое-то время может компенсировать.

—по вероятности возникновения:

- весьма вероятная угроза;
- вероятная угроза;
- маловероятная угроза.

—по причинам появления:

- стихийные бедствия;
- преднамеренные действия.

—по характеру нанесенного ущерба:

- материальный;
- моральный;

—по характеру воздействия:

- активные;
- пассивные.

—по отношению к объекту:

- внутренние;
- внешние.

Источниками внешних угроз являются:

- недобросовестные конкуренты;
- преступные группировки и формирования;
- отдельные лица и организации административно-управленческого аппарата.

Источниками внутренних угроз могут быть:

- администрация предприятия;
- персонал;
- технические средства обеспечения производственной и трудовой деятельности.

Соотношение внешних и внутренних угроз на усредненном уровне можно охарактеризовать так:

- 82% угроз совершается собственными сотрудниками фирмы при их прямом или опосредованном участии;
- 17% угроз совершается извне — внешние угрозы;
- 1% угроз совершается случайными лицами.

Угроза — это потенциальные или реальные действия, приводящие к моральному или материальному ущербу.

1.4. Действия, приводящие к неправомерному овладению конфиденциальной информацией [^]

Отношение объекта (фирма, организация) и субъекта (конкурент, злоумышленник) в информационном процессе с противоположными интересами можно рассматривать с позиции активности в действиях, приводящих к овладению конфиденциальными сведениями. В этом случае возможны такие ситуации:

- владелец (источник) не принимает никаких мер к сохранению конфиденциальной информации, что позволяет злоумышленнику легко получить интересующие его сведения;
- источник информации строго соблюдает меры информационной безопасности, тогда злоумышленнику приходится прилагать значительные усилия к осуществлению доступа к охраняемым сведениям, используя для этого всю совокупность способов несанкционированного проникновения: легальное или нелегальное, заходовое или беззаходовое;
- промежуточная ситуация — это утечка информации по техническим каналам, при которой источник еще не знает об этом (иначе он принял бы меры защиты), а злоумышленник легко, без особых усилий может их использовать в своих интересах.

В общем факт получения охраняемых сведений злоумышленниками или конкурентами называют утечкой. Однако одновременно с этим в значительной части за конодательных актов, законов, кодексов, официальных материалов используются и такие понятия, как разглашение сведений и несанкционированный доступ к конфиденциальной информации (рис. 7).

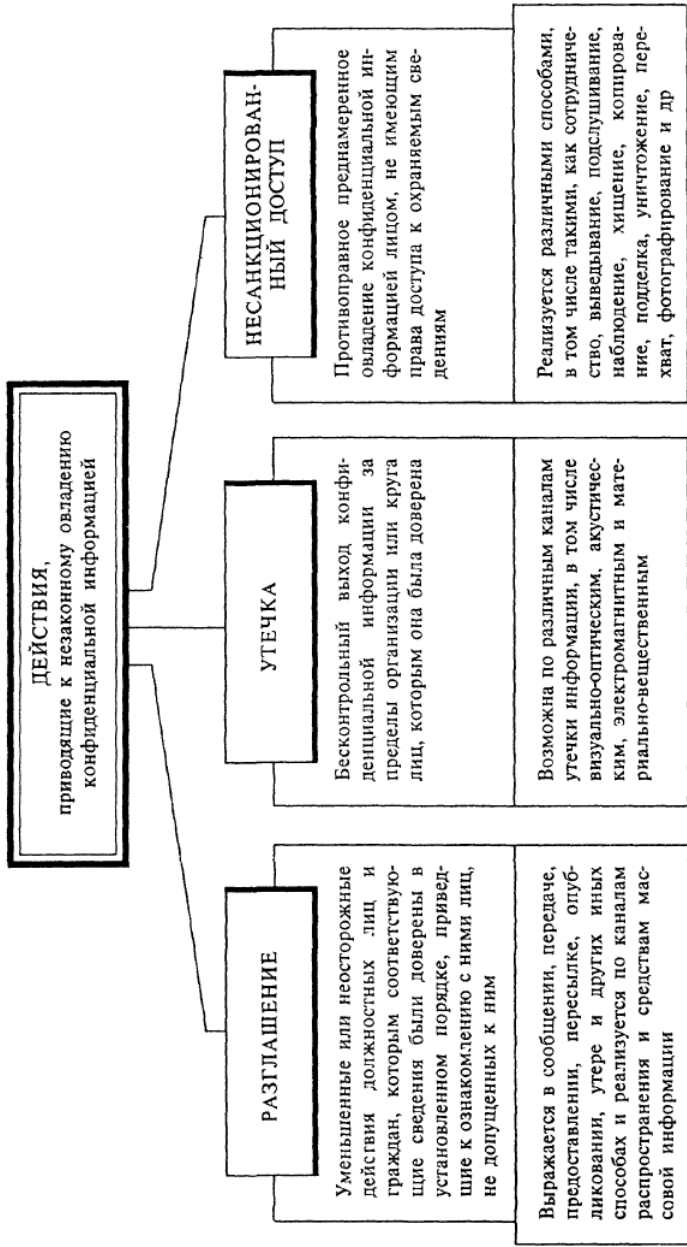


Рис. 7

1. Разглашение — это умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним.

Разглашение выражается в сообщении, передаче, предоставлении, пересылке, опубликовании, утере и в других формах обмена и действий с деловой и научной информацией. Реализуется разглашение по формальным и неформальным каналам распространения информации. К формальным коммуникациям относятся деловые встречи, совещания, переговоры и тому подобные формы общения: обмен официальными деловыми и научными документами средствами передачи официальной информации (почта, телефон, телеграф и т. д.). Неформальные коммуникации включают личное общение (встречи, переписка), выставки, семинары, конференции и другие массовые мероприятия, а также средства массовой информации (печать, газет, интервью, радио, телевидение). Как правило, причиной разглашения конфиденциальной информации является недостаточное знание сотрудниками правил защиты коммерческих секретов и непонимание (или недопонимание) необходимости их тщательного соблюдения. Тут важно отметить, что субъектом в этом процессе выступает источник (владелец) охраняемых секретов.

Следует отметить информационные особенности этого действия. Информация содержательная, осмысленная, упорядоченная, аргументированная, объемная и доводится зачастую в реальном масштабе времени. Часто имеется возможность диалога. Информация ориентирована в определенной тематической области и документирована. Для получения интересующей злоумышленника информации последний затрачивает практически минимальные усилия и использует простые легальные технические средства (диктофоны, видеомониторинг).

2. Утечка — это бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена.

Утечка информации осуществляется по различным техническим каналам. Известно, что информация вообще переносится или передается либо энергией, либо веществом. Это либо акустическая волна (звук), либо электромагнитное излучение, либо лист бумаги (написанный текст) и др. С учетом этого можно утверждать, что по физической природе возможны следующие пути переноса информации: световые лучи, звуковые волны,

электромагнитные волны, материалы и вещества. Соответственно этому классифицируются и каналы утечки информации на визуально-оптические, акустические, электромагнитные и материально-вещественные. Под каналом утечки информации принято понимать физический путь от источника конфиденциальной информации к злоумышленнику, посредством которого последний может получить доступ к охраняемым сведениям. Для образования канала утечки информации необходимы определенные пространственные, энергетические и временные условия, а также наличие на стороне злоумышленника соответствующей аппаратуры приема, обработки и фиксации информации.

3. Несанкционированный доступ — это противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым секретам.

Несанкционированный доступ к источникам конфиденциальной информации реализуется различными способами: от инициативного сотрудничества, выражающегося в активном стремлении «продать» секреты, до использования различных средств проникновения к коммерческим секретам. Для реализации этих действий злоумышленнику приходится часто проникать на объект или создавать вблизи него специальные посты контроля и наблюдения — стационарных или в подвижном варианте, оборудованных самыми современными техническими средствами.

Если исходить из комплексного подхода к обеспечению информационной безопасности, то такое деление ориентирует на защиту информации как от разглашения, так и от утечки по техническим каналам и от несанкционированного доступа к ней со стороны конкурентов и злоумышленников.

Такой подход к классификации действий, способствующих неправомерному овладению конфиденциальной информацией, показывает многогранность угроз и многоаспектность защитных мероприятий, необходимых для обеспечения комплексной информационной безопасности.

С учетом изложенного остается рассмотреть вопрос, какие условия способствуют неправомерному овладению конфиденциальной информацией. В литературе (*Ярочкин В.И. Предприниматель и безопасность. В 2-х ч.*) указываются следующие условия:

- разглашение (излишняя болтливость сотрудников) — 32%;
- несанкционированный доступ путем подкупа и склонения к сотрудничеству со стороны конкурентов и преступных

группировок — 24%;

- отсутствие на фирме надлежащего контроля и жестких условий обеспечения информационной безопасности — 14%;
- традиционный обмен производственным опытом — 12%;
- бесконтрольное использование информационных систем — 10%;
- наличие предпосылок возникновения среди сотрудников конфликтных ситуаций — 8%;

А также отсутствие высокой трудовой дисциплины, психологическая несовместимость, случайный подбор кадров, слабая работа службы кадров по сплочению коллектива.

Среди форм и методов недобросовестной конкуренции на ходят наибольшее распространение:

- экономическое подавление, выражающееся в срыве сделок и иных соглашениях (48%), парализации деятельности фирмы (31%), компрометации фирмы (11%), шантаже руководителей фирмы (10%);
- физическое подавление: ограбления и разбойные нападения на офисы, склады, грузы (73%), угрозы физической расправы над руководителями фирмы и ведущими специалистами (22%), убийства и захват заложников (5%);
- информационное воздействие: подкуп сотрудников (43%), копирование информации (24%), проникновение в базы данных (18%), продажа конфиденциальных документов (10%), подслушивание телефонных переговоров и переговоров в помещениях (5%), а также ограничение доступа к информации, дезинформация;
- финансовое подавление включает такие понятия, как инфляция, бюджетный дефицит, коррупция, хищение финансов, мошенничество;
- психическое давление может выражаться в виде хулиганских выходок, угрозы и шантажа, энерго-информационного воздействия.

Основными угрозами информации являются ее разглашение, утечка и несанкционированный доступ к ее источникам.

Каждому из условий неправомерного овладения

конфиденциальной информацией можно поставить в соответствие определенные каналы, определенные способы защитных действий и определенные классы средств защиты или противодействия. Совокупность определений, каналов, способов и средств представ- ляется в виде следующей схемы (рис. 8).

Выводы:

Изложенное в этой главе можно кратко сформулировать так.

1. Информация — это ресурс. Потеря конфиденциальной информации приносит моральный или материальный ущерб.
2. Условия, способствующие неправомерному овладению конфиденциальной информацией, сводятся к ее разглашению, утечке и несанкционированному доступу к ее источникам.
3. В современных условиях безопасность информационных ресурсов может быть обеспечена только комплексной системой защиты информации.
4. Комплексная система защиты информации должна быть: непрерывной, плановой, целенаправленной, конкретной, активной, надежной.
5. Система защиты информации должна опираться на систему видов собственного обеспечения, способного реализовать ее функционирование не только в повседневных условиях, но и в критических ситуациях.

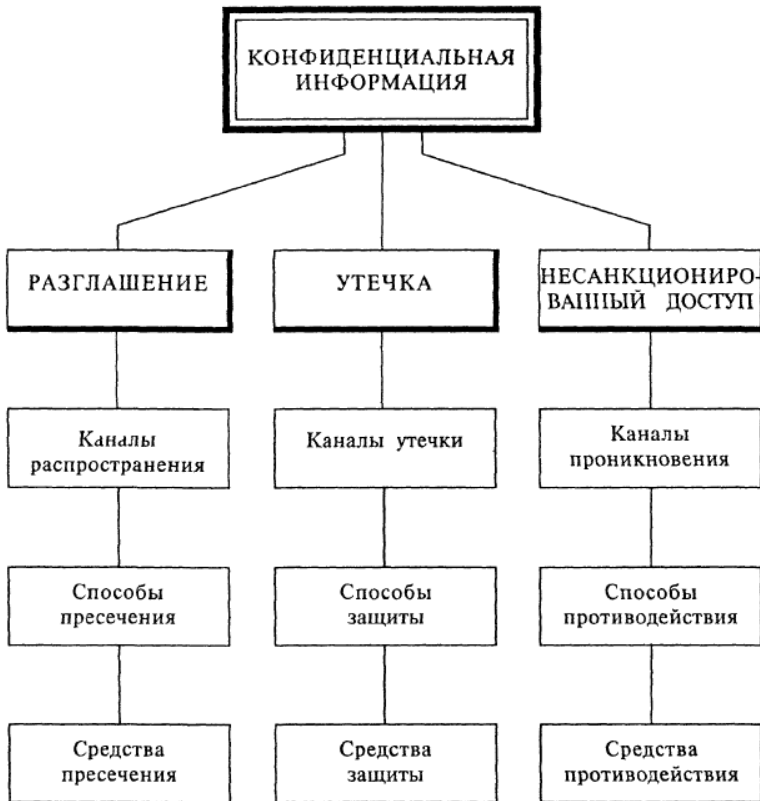


Рис. 8

Глава 2 НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ [^]

Подальше положишь — поближе возьмешь

Направления обеспечения информационной безопасности — это нормативно-правовые категории, ориентированные на обеспечение комплексной защиты информации от внутренних и внешних угроз.

Постулаты безопасности

1. Если не уверен в безопасности, считай, что опасность существует реально.
2. Безопасности бесплатной не бывает.
3. Безопасности не бывает много.
4. Безопасность должна быть только комплексной.
5. Комплексная безопасность может быть обеспечена только системой безопасности.
6. Никакая система безопасности не обеспечивает требуемого уровня без надлежащей подготовки руководителей, сотрудников и клиентов.
7. В безопасности должен быть заинтересован каждый.

Направления обеспечения безопасности вообще рассматриваются как нормативно-правовые категории, определяющие комплексные меры защиты информации на государственном уровне, на уровне предприятия и организации, на уровне отдельной личности.

С учетом сложившейся практики обеспечения информационной безопасности выделяют следующие направления защиты информации:

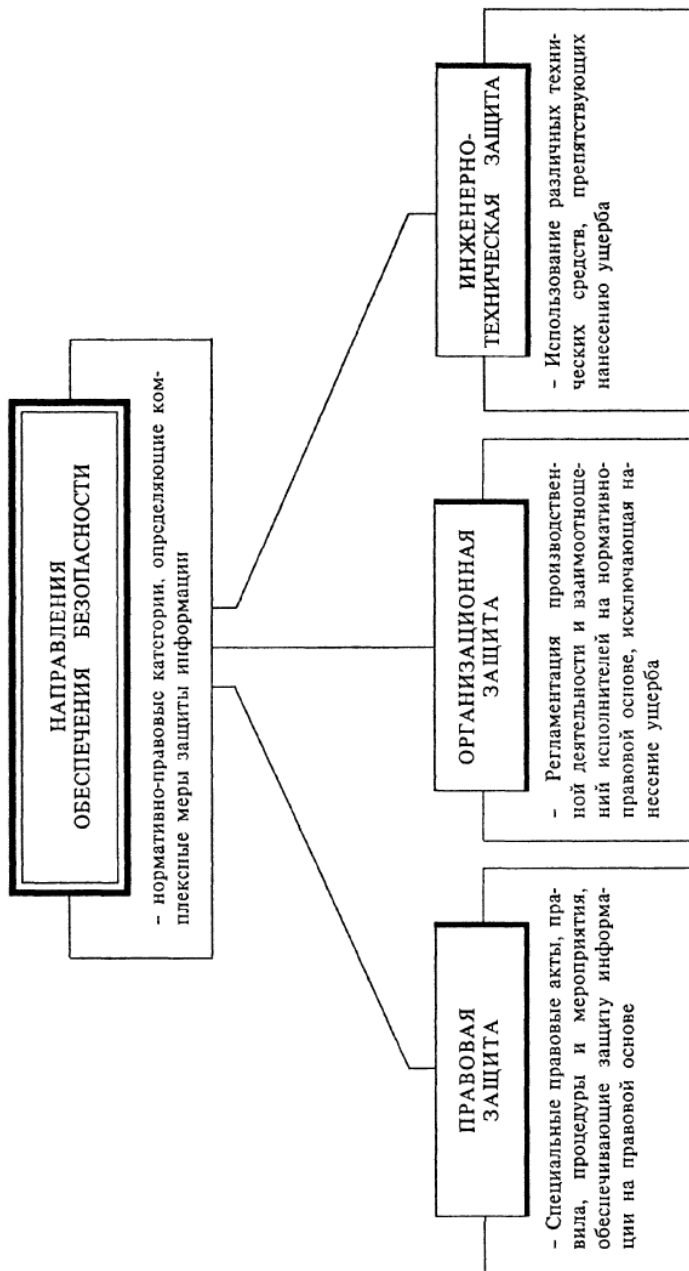


Рис. 9

- правовая защита — это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;
- организационная защита — это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какому-либо ущерба исполнителям;
- инженерно-техническая защита — это использование различных технических средств, препятствующих нанесению ущерба коммерческой деятельности (рис. 9).

Кроме этого, защитные действия, ориентированные на обеспечение информационной безопасности, могут быть охарактеризованы целым рядом параметров, отражающих, помимо направлений, ориентацию на объекты защиты, характер угроз, способы действий, их распространенность, охват и масштабность (рис. 10).

Так, по характеру угроз защитные действия ориентированы на защиту информации от разглашения, утечки и несанкционированного доступа. По способам действий их можно подразделить на предупреждение, выявление, обнаружение, пресечение и восстановление ущерба или иных убытков. По охвату защитные действия могут быть ориентированы на территорию, здание, помещение, аппаратуру или отдельные элементы аппаратуры. Масштабность защитных мероприятий характеризуется как объектовая, групповая или индивидуальная защита. Например, защита автономной ПЭВМ в режиме индивидуального пользования.

2.1. Правовая защита [^]

Как известно, право — это совокупность общеобязательных правил и норм поведения, установленных или санкционированных государством в отношении определенных сфер жизни и деятельности государственных органов, предприятий (организаций) и населения (отдельной личности).

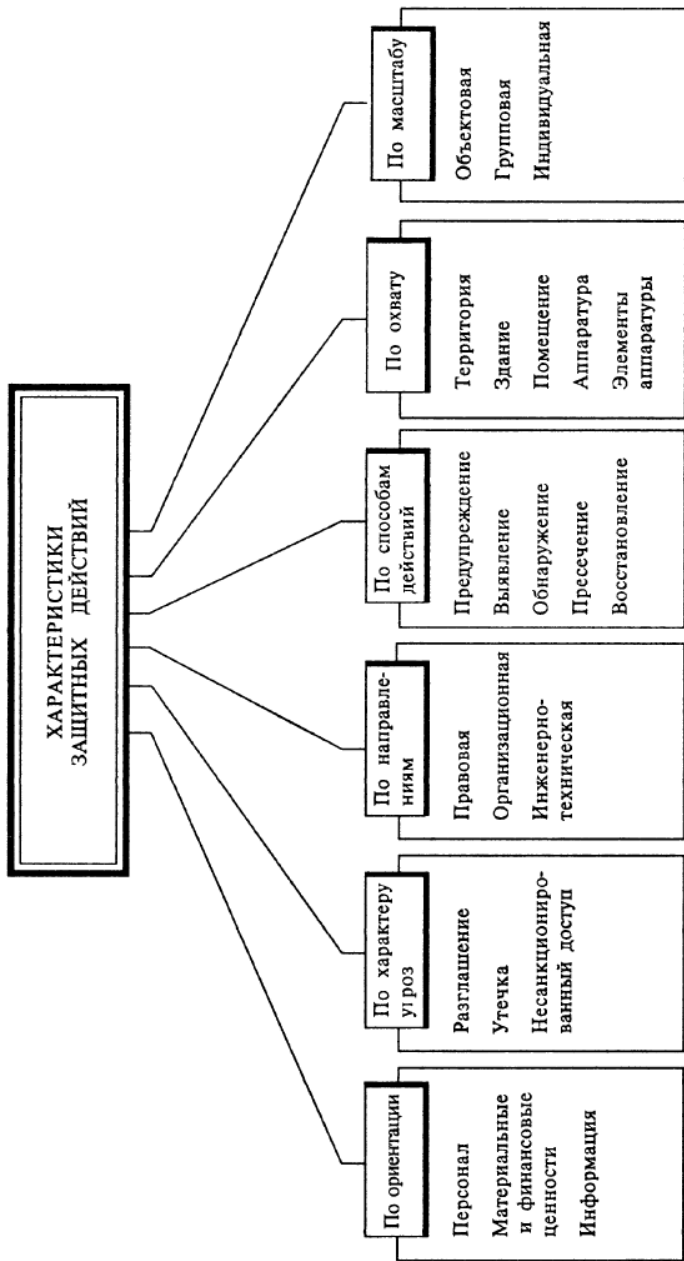


Рис. 10

Правовая защита информации как ресурса признана на международном, государственном уровне и определяется межгосударственными договорами, конвенциями, декларациями и реализуется патентами, авторским правом и лицензиями на их защиту. На государственном уровне правовая защита регулируется государственными и ведомственными актами (рис. 11).

В нашей стране такими правилами (актами, нормами) являются Конституция, законы Российской Федерации, гражданское, административное, уголовное право, изложенные в соответствующих кодексах. Что касается ведомственных нормативных актов, то они определяются приказами, руководствами, положениями и инструкциями, издаваемыми ведомствами, организациями и предприятиями, действующими в рамках определенных структур (рис. 12).

Современные условия требуют и определяют необходимость комплексного подхода к формированию законодательства по защите информации, его состава и содержания, соотнесения его со всей системой законов и правовых актов Российской Федерации.

Требования информационной безопасности должны органически включаться во все уровни законодательства, в том числе и в конституционное законодательство, основные общие законы, законы по организации государственной системы управления, специальные законы, ведомственные правовые акты и другие. В литературе приводится такая структура правовых актов, ориентированных на правовую защиту информации.

Первый блок — конституционное законодательство. Нормы, касающиеся вопросов информатизации и защиты информации, входят в него как составные элементы.

Второй блок — общие законы, кодексы (о собственности, о недрах, о земле, о правах граждан, о гражданстве, о налогах, об антимонопольной деятельности), которые включают нормы по вопросам информатизации и информационной безопасности.

Третий блок — законы об организации управления, касающиеся отдельных структур хозяйства, экономики, системы государственных органов и определяющие их статус. Они включают отдельные нормы

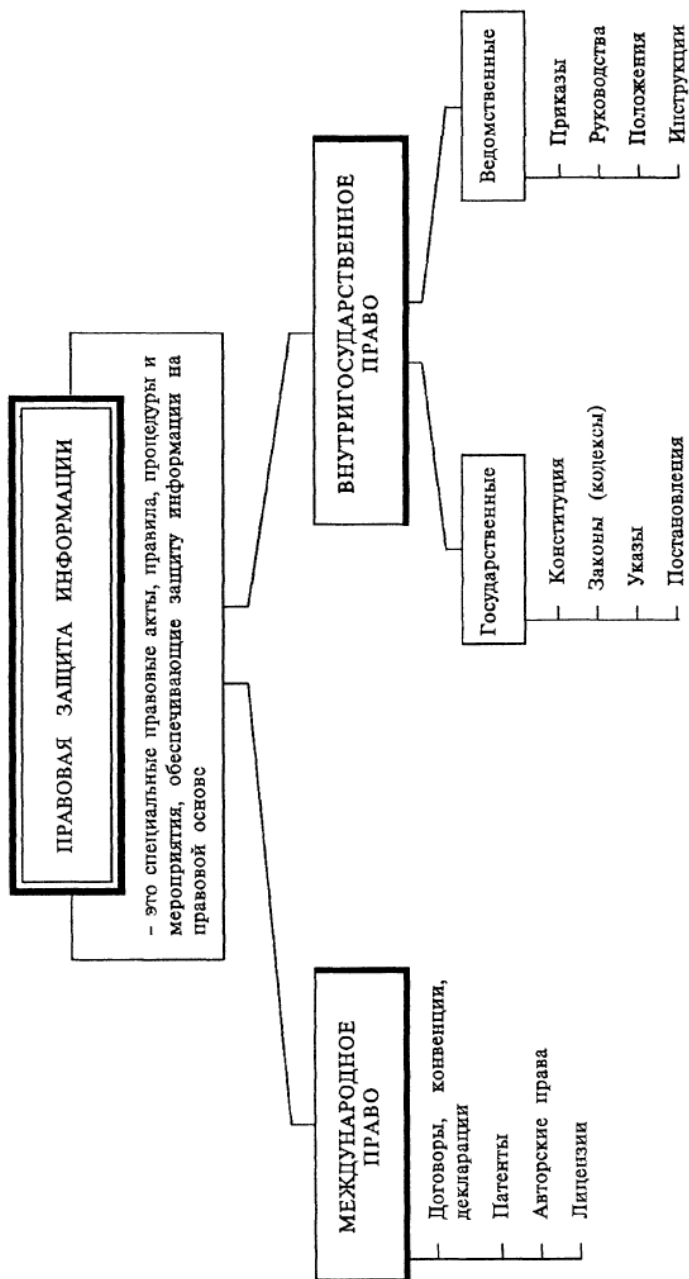


Рис. 11

по вопросам защиты информации. Наряду с общими вопросами информационного обеспечения и защиты информации конкретного органа эти нормы должны устанавливать его обязанности по формированию, актуализации и безопасности информации, представляющей общегосударственный интерес.

Четвертый блок — специальные законы, полностью относящиеся к конкретным сферам отношений,

СТРУКТУРА ЗАКОНОДАТЕЛЬСТВА РОССИИ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

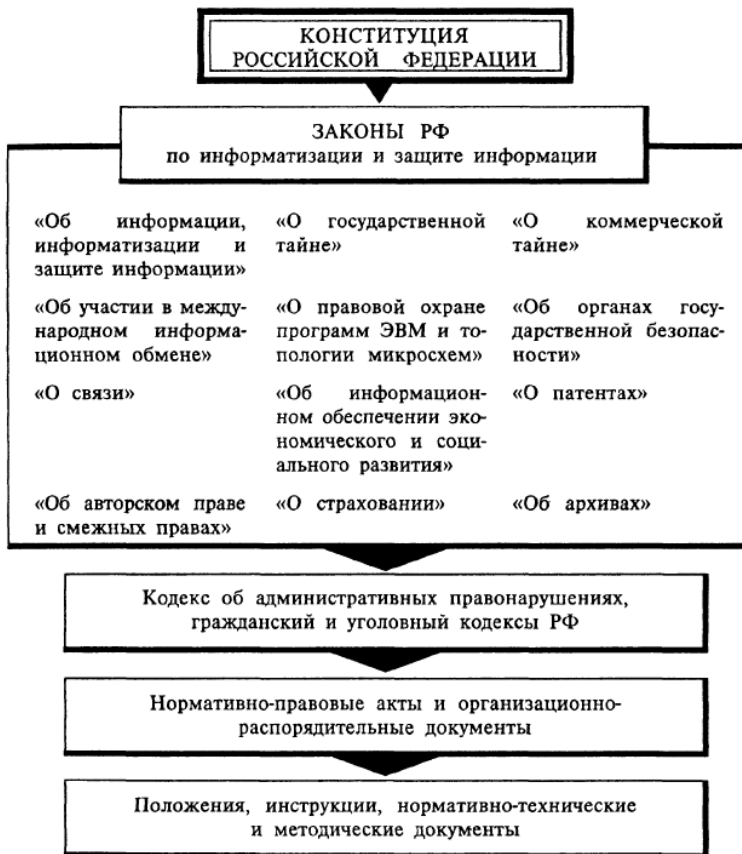


Рис. 12

отраслям хозяйства, процессам. В их число входит и Закон РФ «Об информации, информатизации и защите информации». Именно состав и содержание этого блока законов и создает специальное законодательство как основу правового обеспечения информационной безопасности.

Пятый блок — законодательство субъектов Российской Федерации, касающееся защиты информации.

Шестой блок — подзаконные нормативные акты по защите информации.

Седьмой блок — это правоохранительное законодательство России, содержащее нормы об ответственности за правонарушения в сфере информатизации.

Специальное законодательство в области безопасности информационной деятельности может быть представлено совокупностью законов. В их составе особое место принадлежит базовому Закону «Об информации, информатизации и защите информации», который закладывает основы правового определения всех важнейших компонентов информационной деятельности:

- информации и информационных систем;
- субъектов — участников информационных процессов;
- правоотношений производителей — потребителей информационной продукции;
- владельцев (обладателей, источников) информации — обработчиков и потребителей на основе отношений собственности при обеспечении гарантий интересов граждан и государства.

Этот закон определяет основы защиты информации в системах обработки и при ее использовании с учетом категорий доступа к открытой информации и к информации с ограниченным доступом. Этот закон содержит, кроме того, общие нормы по организации и ведению информационных систем, включая банки данных государственного назначения, порядка государственной регистрации, лицензирования, сертификации, экспертизы, а также общие принципы защиты и гарантий прав участников информационного процесса.

В дополнение к базовому закону в мае 1992 г. Были приняты Законы «О правовой охране программ для электронно-вычислительных машин и баз данных» и «О правовой охране топологии интегральных микросхем». Оба закона устанавливают охрану соответствующих объектов с помощью норм авторского права, включая в перечень объектов авторского права наряду с

традиционными базами данных топологии интегральных микросхем и программы для ЭВМ.

Вопросы правового режима информации с ограниченным доступом реализуются в двух самостоятельных законах о государственной и коммерческой (проект) тайнах. Кроме того, этот аспект раскрывается и в Гражданском кодексе РФ статьей 139 «Служебная и коммерческая тайна».

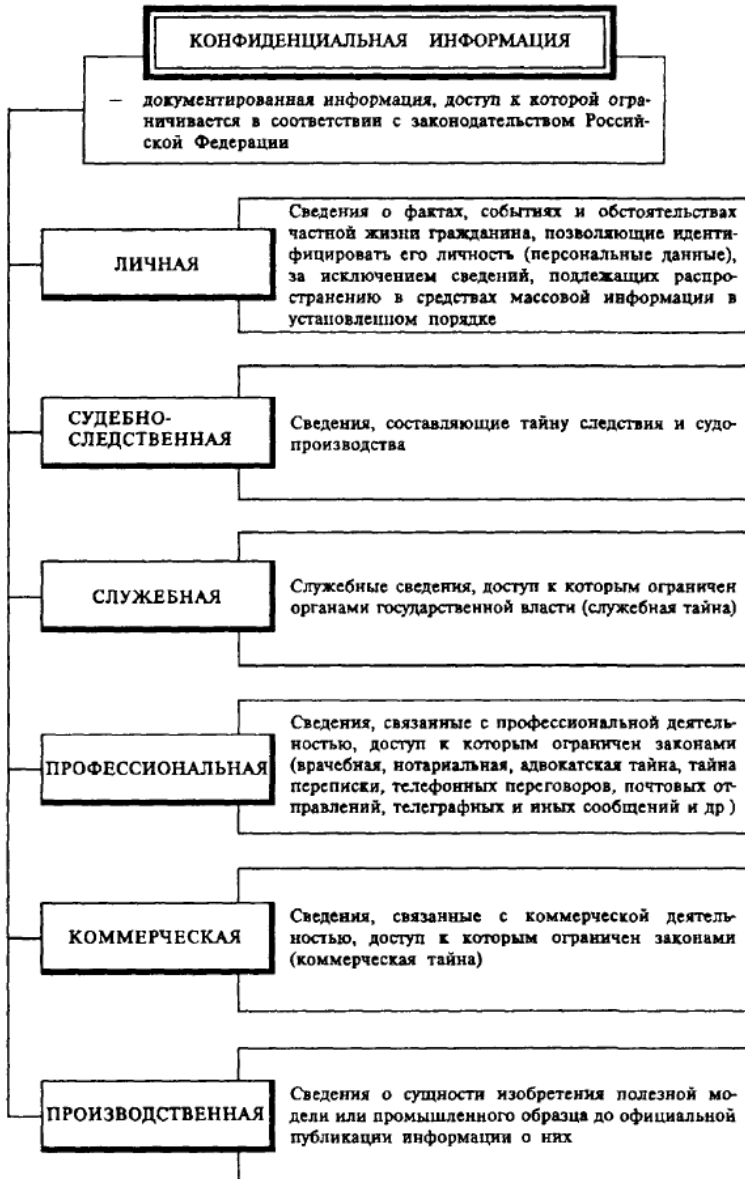
1. Информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности. Сведения, которые не могут составлять служебную или коммерческую тайну, определяются законом и иными правовыми актами.
2. Информация, составляющая служебную или коммерческую тайну, защищается способами, предусмотренными настоящим кодексом и другими законами.

Вторая часть статьи 139 определяет правовые основы ответственности за несанкционированное получение информации или причинение ущерба. Звучит это так:

«Лица, незаконными методами получившие информацию, которая составляет служебную или коммерческую тайну, обязаны возместить причиненные убытки. Такая же обязанность возлагается на работников, разгласивших служебную или коммерческую тайну вопреки трудовому договору, в том числе контракту, и на контрагентов, сделавших это вопреки гражданско-правовому договору».

Указ Президента РФ от 6 марта 1997 г. № 188 определяет понятие и содержание конфиденциальной информации (см. таблицу 1)

Таблица 1



Таким образом, правовая защита информации обеспечивается нормативно-законодательными актами, представляющими собой по уровню иерархическую систему от Конституции РФ до функциональных обязанностей и контракта отдельного конкретного исполнителя, определяющих перечень сведений, подлежащих охране, и меры ответственности за их разглашение.

Одним из новых для нас направлений правовой защиты является страховое обеспечение. Оно предназначено для защиты собственника информации и средств ее обработки как от традиционных угроз (кражи, стихийные бедствия), так и от угроз, возникающих в ходе работы с информацией. К ним относятся: разглашение, утечка и несанкционированный доступ к конфиденциальной информации.

Целью страхования является обеспечение страховой защиты физических и юридических лиц от страховых рисков в виде полного или частичного возмещения ущерба и потерь, причиненных стихийными бедствиями, чрезвычайными происшествиями в различных областях деятельности, противоправными действиями со стороны конкурентов и злоумышленников путем выплат денежной компенсации или оказания сервисных услуг (ремонт, восстановление) при наступлении страхового события.

В основе российского страхового законодательства лежит Закон РФ «О страховании». Он призван гарантировать защиту интересов страхователей, определять единые положения по организации страхования и принципы государственного регулирования страховой деятельности.

Закон «О страховании» дает следующее понятие страхования: «Страхование представляет собой отношения по защите имущественных интересов физических и юридических лиц при наступлении определенных событий (страховых случаев) за счет денежных фондов, формируемых из уплачиваемых ими страховых взносов».

Действия по защите информации от утечки по техническим каналам регламентируются следующими правовыми документами:

1. ГОСТ 29339-92 «Информационная технология. Защита информации от утечки за счет ПЭМИН при ее обработке СВТ». (ПЭМИН — побочные электромагнитные излучения и наводки.).
2. ГОСТ Р 50752 «Информационная технология. Защита

информации от утечки за счет ПЭМИН при ее обработке средствами вычислительной техники. Методы испытаний».

3. Нормы эффективности и защиты АСУ и ЭВМ от утечки информации за счет ПЭМИН.
4. Специальные требования и рекомендации по защите объектов ЭВТИ и III категории от утечки информации за счет ПЭМИН.

Действия по защите информации от несанкционированного доступа (НСД) регламентируют Постановление Правительства РФ от 15.09.93 № 912-51 «Положение о государственной системе защиты информации от иностранной технической разведки и от утечки по техническим каналам», а также Указы Президента РФ «О создании государственной технической комиссии при Президенте РФ» (от 05.01.92 № 9); «О защите информационно-телекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам связи» (от 08.05.93 № 644); «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации» (от 03.04.95 № 334); «Положение о государственной системе защиты информации в Российской Федерации».

Правовыми документами являются и государственные стандарты на информационную деятельность с учетом обеспечения ее безопасности, в частности ГОСТ Р 50739-95 «СВТ. Защита от НСД к информации»; ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»; ГОСТ Р.34.10-94 «Процедуры выработки и проверки электронной подписи на базе асимметричного криптографического алгоритма»; ГОСТ Р.34.11-94 «Функция хэширования»; ГОСТ Р.В.50170-92 «Противодействие ИТР. Термины и определения».

Опираясь на государственные правовые акты и учитывая ведомственные интересы на уровне конкретного предприятия (фирмы, организации), разрабатываются собственные нормативно-правовые документы, ориентированные на обеспечение информационной безопасности. К таким документам относятся:

- Положение о сохранении конфиденциальной информации;
- Перечень сведений, составляющих конфиденциальную информацию;
- Инструкция о порядке допуска сотрудников к сведениям,

- составляющим конфиденциальную информацию;
- Положение о специальном делопроизводстве и документообороте;
- Перечень сведений, разрешенных к опубликованию в открытой печати;
- Положение о работе с иностранными фирмами и их представителями;
- Обязательство сотрудника о сохранении конфиденциальной информации;
- Памятка сотруднику о сохранении коммерческой тайны.

Указанные нормативные акты направлены на предупреждение случаев неправомерного оглашения (разглашения) секретов на правовой основе, и в случае их нарушения должны приниматься соответствующие меры воздействия.

В зависимости от характера информации, ее доступности для заинтересованных потребителей, а также экономической целесообразности конкретных защитных мер могут быть избраны следующие формы защиты информации:

- патентование;
- авторское право;
- признание сведений конфиденциальными;
- товарные знаки;
- применение норм обязательственного права.

В таблице 2а приводятся некоторые характеристики этих форм и анализируется взаимосвязь между ними, а в таблице 2б приведены определения и основные параметры коммерческой тайны.

Существуют определенные различия между авторским правом и коммерческой тайной. Авторское право

Таблица 2а

Взаимосвязь патентов и коммерческой тайны

| Хактеристики | Патенты | Коммерческая тайна |
|-------------------------|--|--|
| Объект защиты | Специфический и четко определенный документ | Применима к широкому спектру интеллектуальной собственности и деловой информации |
| Требования к информации | Информация должна быть: полезной, новой, неочевидной | Информация должна быть: - потенциально полезной, не должна |

| | | |
|-----------------------------|---|--|
| | | быть общеизвестной, не обязательно должна быть новой и неочевидной |
| Степень определенности | Четко определена в заявке | Часто трудно четко определить |
| Необходимость опубликования | Строго необходима. Публикуется обязательно. | Любое обнародование должно быть под контролем и ограничено в неизвестной степени (храниться в тайне) |
| Порядок защиты | Определяется узким, но четким статусом Предоставляется монополия | Определяется в зависимости от обстоятельств. Реализуется только от недобросовестной конкуренции |
| Продолжительность защиты | 15 - 20 лет с момента опубликования | Практически не ограничена |
| Стоимость | По получению патента | Защита от утечки и использования информации другими лицами |
| Стоимость риска | Недействительность по истечении срока | Независимое открытие другими лицами |

защищает только форму выражения идеи. Коммерческая тайна относится непосредственно к содержанию. Авторское право защищает от копирования независимо от конфиденциальных отношений с владельцем. К авторскому праву прибегают при широкой публикации своей информации, в то время как коммерческую тайну держат в секрете. Очевидно, что по сравнению с патентом и авторским правом, коммерческая и производственная тайны являются наиболее удобными, надежными и гибкими формами защиты информации.

Помимо вышеизложенных форм правовой защиты и права принадлежности информации находит широкое распространение официальная передача права на пользование ею в виде лицензии. Лицензия — это разрешение, выдаваемое государством на

проведение некоторых видов хозяйственной деятельности, включая внешнеторговые операции (ввоз и вывоз) и предоставление права использовать защищенные патентами изобретения, технологии, методики. Лицензионные разрешения предоставляются на определенное время и на определенные виды товаров.

Таблица 26

Коммерческая тайна

Коммерческая тайна — не являющиеся государственными секретами сведения, связанные с производством, технологией, управлением, финансами и другой деятельностью, разглашение, утечка и несанкционированный доступ к которой может нанести ущерб их владельцам.

| Определения | Содержание |
|----------------|--|
| СУБЪЕКТ | Предприятия, организации, коллективы, граждане |
| ОБЪЕКТ | Понятие применимо к широкому спектру интеллектуальной и промышленной собственности |
| ХАРАКТЕРИСТИКИ | 1. Активный ресурс 2. Конфиденциальная информация 3. Особая форма собственности 4. Товар рыночной новизны |
| ЦЕННОСТЬ | Реально (потенциально) создает преимущества в конкурентной борьбе |
| ТРЕБОВАНИЯ | 1. Потенциально полезная 2. Не общеизвестная |
| СРОК ДЕЙСТВИЯ | Определяется жизненным циклом товара |
| ЗАЩИТА | 1. Правовая 2. Организационная 3. Инженерно-техническая |

К коммерческой тайне не относятся:

- охраняемые государством сведения;
- общеизвестные на законных основаниях сведения;
- общедоступные сведения, патенты, товарные знаки;
- сведения о негативной стороне деятельности;

- учредительные документы и сведения о хозяйственной деятельности.

На все эти формы защиты интеллектуальной собственности имеются соответствующие законы РФ — закон о патентах, закон об авторском праве, проект закона о коммерческой тайне, закон о товарных знаках и другие.

Создавая систему информационной безопасности, необходимо четко понимать, что без правового обеспечения защиты информации любые последующие претензии с вашей стороны к недобросовестному сотруднику, клиенту, конкуренту и должностному лицу окажутся просто беспочвенными.

Если перечень сведений конфиденциального характера не доведен своевременно до каждого сотрудника (естественно, если он допущен по должностным обязанностям) в письменном виде, то сотрудник, укравший важную информацию в нарушение установленного порядка работы с ней, скорее всего разведет руками: мол, откуда мне это знать! В этом случае никакие инстанции, вплоть до судебных, не смогут Вам помочь.

Правовые нормы обеспечения безопасности и защиты информации на конкретном предприятии (фирме, организации) отражаются в совокупности учредительных, организационных и функциональных документов.

Требования обеспечения безопасности и защиты информации отражаются в Уставе (учредительном договоре) в виде следующих положений:

- предприятие имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, требовать от своих сотрудников обеспечения их сохранности и защиты от внутренних и внешних угроз;
- предприятие обязано обеспечить сохранность конфиденциальной информации.

Такие требования дают право администрации предприятия:

- создавать организационные структуры по защите конфиденциальной информации;
- издавать нормативные и распорядительные документы, определяющие порядок выделения сведений конфиденциального характера и механизмы их защиты;
- включать требования по защите информации в договоры по всем видам хозяйственной деятельности;
- требовать защиты интересов предприятия со стороны

- государственных и судебных инстанций;
- распоряжаться информацией, являющейся собственностью предприятия, в целях извлечения выгоды и недопущения экономического ущерба коллективу предприятия и собственнику средств производства;
 - разработать «Перечень сведений конфиденциальной информации». Требования правовой обеспеченности защиты информации предусматриваются в коллективном договоре. Коллективный договор должен содержать следующие требования:

Раздел «Предмет договора»

Администрация предприятия (в том числе и администрация самостоятельных подразделений) обязуется обеспечить разработку и осуществление мероприятий по определению и защите конфиденциальной информации.

Трудовой коллектив принимает на себя обязательства по соблюдению установленных на предприятии требований по защите конфиденциальной информации.

Администрация обязана учесть требования защиты конфиденциальной информации в правилах внутреннего распорядка.

Раздел «Кадры. Обеспечение дисциплины труда»

Администрация обязуется: нарушителей требований по защите коммерческой тайны привлекать к административной и уголовной ответственности в соответствии с действующим законодательством.

Правила внутреннего трудового распорядка для рабочих и служащих предприятия целесообразно дополнить следующими требованиями.

Раздел «Порядок приема и увольнения рабочих и служащих»

- При поступлении рабочего или служащего на работу или переводе его в установленном порядке на другую работу, связанную с конфиденциальной информацией предприятия, а также при увольнении администрация обязана проинструктировать работника или служащего по правилам сохранения коммерческой тайны с оформлением письменного обязательства о ее

неразглашении.

- Администрация предприятия вправе принимать решение об отстранении от работ лиц, которые нарушают установленные требования по защите конфиденциальной информации.

Раздел «Основные обязанности рабочих и служащих»

Рабочие и служащие обязаны соблюдать требования нормативных документов по защите конфиденциальной информации предприятия.

Раздел «Основные обязанности администрации»

Администрация предприятия, руководители подразделений обязаны:

- обеспечить строгое сохранение конфиденциальной информации, постоянно осуществлять организаторскую и воспитательно-профилактическую работу, направленную на защиту секретов предприятия;
- включить в должностные инструкции и положения обязанности по сохранению конфиденциальной информации;
- неуклонно выполнять требования Устава, коллективного договора, трудовых договоров, правил внутреннего трудового распорядка и других организационных и хозяйственных документов в части обеспечения экономической и информационной безопасности.

Обязательства конкретного сотрудника, рабочего или служащего в части защиты информации обязательно должны быть оговорены в трудовом договоре (контракте). В соответствии с КЗоТ (гл. III) при заключении трудового договора трудящийся обязуется выполнять определенные требования, действующие на данном предприятии. Независимо от формы заключения договора (устного или письменного) подпись трудящегося на приказе о приеме на работу подтверждает его согласие с условиями договора (КЗоТ РФ ст. 18).

Требования по защите конфиденциальной информации могут быть оговорены в тексте договора, если договор заключается в письменной форме. Если же договор заключается в устной форме, то действуют требования по защите информации, вытекающие из

нормативно-правовых документов предприятия. При заключении трудового договора и оформлении приказа о приеме на работу нового сотрудника делается отметка об осведомленности его с порядком защиты информации предприятия. Это создает необходимый элемент включения данного лица в механизм обеспечения информационной безопасности.

Использование договоров о неразглашении тайны — вовсе не самостоятельная мера по ее защите. Не следует думать, что после подписания такого соглашения с новым сотрудником тайна будет сохранена. Это только предупреждение сотруднику, что в дело вступает система мероприятий по защите информации, и правовая основа к тому, чтобы пресечь его неверные или противоправные действия. Дальше задача — не допустить утраты коммерческих секретов.

Реализация правовых норм и актов, ориентированных на защиту информации на организационном уровне, опирается на те или иные организационно-правовые формы, к числу которых относятся соблюдение конфиденциальности работ и действий, договоры (соглашения) и различные формы обязательного права.

Конфиденциальность — это форма обращения со сведениями, составляющими коммерческую тайну, на основе организационных мероприятий, исключающих неправомерное овладение такими сведениями.

Договоры — это соглашения сторон (двух и более лиц) об установлении, изменении или прекращении взаимных обязательств.

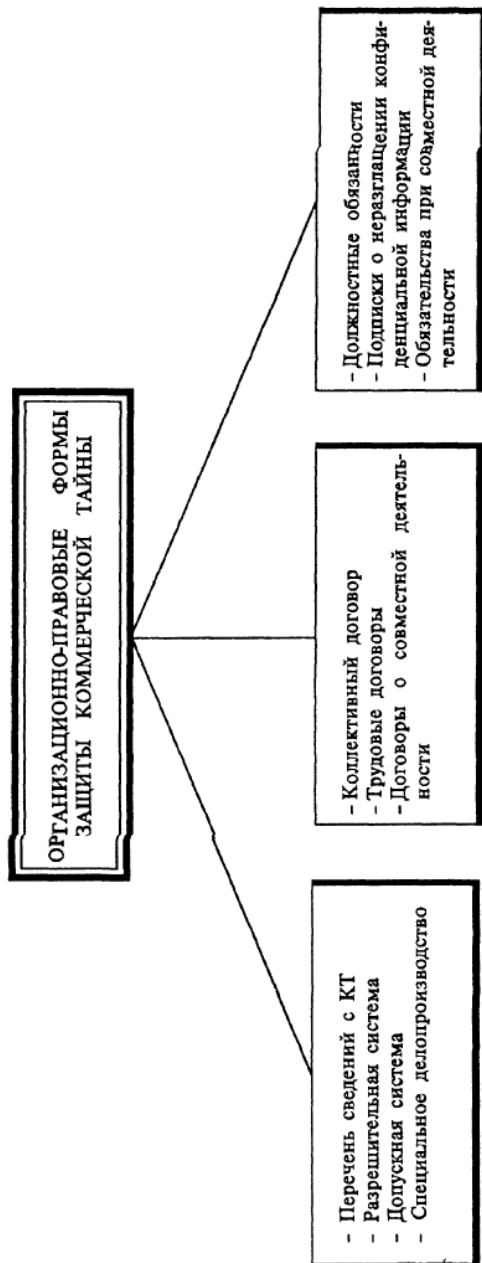


Рис. 13

Обязательство — гражданское правоотношение, в силу которого одна сторона (должник) обязана совершить в пользу другой стороны определенные действия (рис. 13).

Правовое регулирование необходимо для совершенствования механизма предупреждения противоправных действий по отношению к информационным ресурсам, для уточнения и закрепления задач и правомочий отдельных субъектов в сфере предупредительной деятельности, охраны прав и законных интересов граждан и организаций.

Анализ законодательства, регулирующего деятельность субъектов в сфере информационной безопасности, показывает наличие определенных недостатков. Существующие правовые нормы разбросаны по различным нормативным актам, издававшимся в разное время, в разных условиях и на разных уровнях. Действующее законодательство не систематизировано, что создает большие трудности в его использовании на практике.

Правовые меры обеспечения безопасности и защиты информации являются основой порядка деятельности и поведения сотрудников предприятия и определяют меры их ответственности за нарушение установленных норм.

2.2. Организационная защита [^]

Организационная защита — это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз.

Организационная защита обеспечивает:

- организацию охраны, режима, работу с кадрами, с документами;
- использование технических средств безопасности и информационно-аналитическую деятельность по выявлению внутренних и внешних угроз предпринимательской деятельности.

Организационные мероприятия играют существенную роль в создании надежного механизма защиты информации, так как

возможности несанкционированного использования конфиденциальных сведений в значительной мере обуславливаются не техническими аспектами, а злоумышленными действиями, нерадивостью, небрежностью и халатностью пользователей или персонала защиты. Влияния этих аспектов практически невозможно избежать с помощью технических средств. Для этого необходима совокупность организационно-правовых и организационно-технических мероприятий, которые исключали бы (или, по крайней мере, сводили бы к минимуму) возможность возникновения опасности конфиденциальной информации.

К основным организационным мероприятиям можно отнести:

- организацию режима и охраны. Их *цель* — исключение возможности тайного проникновения на территорию и в помещения посторонних лиц; обеспечение удобства контроля прохода и перемещения сотрудников и посетителей; создание отдельных производственных зон по типу конфиденциальных работ с самостоятельными системами доступа; контроль и соблюдение временного режима труда и пребывания на территории персонала фирмы; организация и поддержание надежного пропускного режима и контроля сотрудников и посетителей и др.;
- организацию работы с сотрудниками, которая предусматривает подбор и расстановку персонала, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.;
- организацию работы с документами и документированной информацией, включая организацию разработки и использования документов и носителей конфиденциальной информации, их учет, исполнение, возврат, хранение и уничтожение;
- организацию использования технических средств сбора, обработки, накопления и хранения конфиденциальной информации;
- организацию работы по анализу внутренних и внешних угроз конфиденциальной информации и выработке мер по обеспечению ее защиты;
- организацию работы по проведению систематического

контроля за работой персонала с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей (рис. 14).

В каждом конкретном случае организационные мероприятия носят специфическую для данной организации форму и содержание, направленные на обеспечение безопасности информации в конкретных условиях.

Специфической областью организационных мер является организация защиты ПЭВМ, информационных систем и сетей.

Организация защиты ПЭВМ, информационных систем и сетей определяет порядок и схему функционирования основных ее подсистем, использование устройств и ресурсов, взаимоотношения пользователей между собой в соответствии с нормативно-правовыми требованиями и правилами. Защита информации на основе организационных мер играет большую роль в обеспечении надежности и эффективности, так как несанкционированный доступ и утечка информации чаще всего обусловлены злоумышленными действиями, небрежностью пользователей или персонала. Эти факторы практически невозможно исключить или локализовать с помощью аппаратных и программных средств, криптографии и физических средств защиты. Поэтому совокупность организационных, организационно-правовых и организационно-технических мероприятий, применяемых совместно с техническими методами, имеют цель исключить, уменьшить или полностью устранить потери при действии различных нарушающих факторов.

Организационные средства защиты ПЭВМ и информационных сетей применяются:

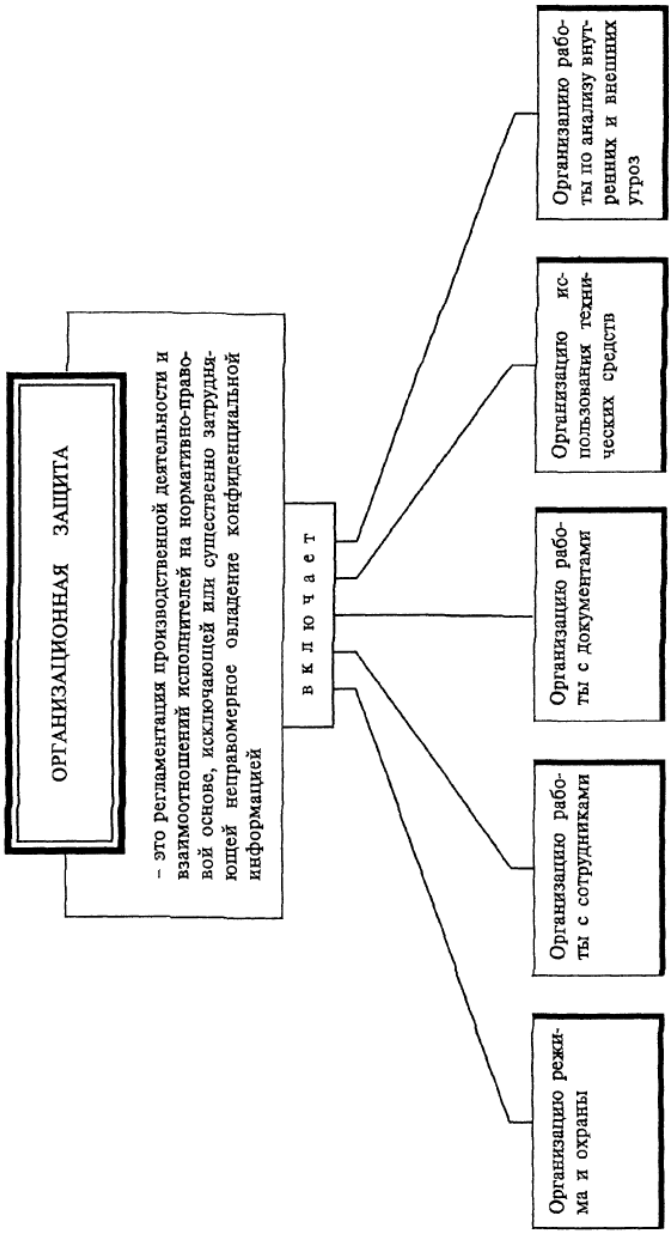


Рис. 14

- при проектировании, строительстве и оборудовании помещений, узлов сети и других объектов информационной системы, исключающих влияние стихийных бедствий, возможность недозволенного проникновения в помещения и др.;
- при подборе и подготовке персонала. В этом случае предусматриваются проверка принимаемых на работу, создание условий, при которых персонал был бы заинтересован в сохранности данных, обучение правилам работы с закрытой информацией, ознакомление с мерами ответственности за нарушение правил защиты и др.;
- при хранении и использовании документов и других носителей (маркировка, регистрация, определение правил выдачи и возвращения, ведение документации и др.);
- при соблюдении надежного пропускного режима к техническим средствам, к ПЭВМ и информационным системам при сменной работе (выделение ответственных за защиту информации в сменах, контроль за работой персонала, ведение (возможно и автоматизированное) журналов работы, уничтожение в установленном порядке закрытых производственных документов);
- при внесении изменений в программное обеспечение (строгое санкционирование, рассмотрение и утверждение проектов изменений, проверка их на удовлетворение требованиям защиты, документальное оформление изменений и др.);
- при подготовке и контроле работы пользователей.

Одним из важнейших организационных мероприятий является создание специальных штатных служб защиты информации в закрытых информационных системах в виде администратора безопасности сети и администратора распределенных баз и банков данных, содержащих сведения конфиденциального характера.

Очевидно, что организационные мероприятия должны четко планироваться, направляться и осуществляться какой-то организационной структурой, каким-то специально созданным для этих целей структурным подразделением, укомплектованным соответствующими специалистами по безопасности предпринимательской деятельности и защите информации.

Зачастую таким структурным подразделением является служба безопасности предприятия (фирмы, организации), на которую

возлагаются следующие общие функции:

- организация и обеспечение охраны персонала, материальных и финансовых ценностей и защиты конфиденциальной информации;
- обеспечение пропускного и внутриобъектового режима на территории, в зданиях и помещениях, контроль соблюдения требований режима сотрудниками, смежниками, партнерами и посетителями;
- руководство работами по правовому и организационному регулированию отношений по защите информации;
- участие в разработке основополагающих документов с целью закрепления в них требований обеспечения безопасности и защиты информации, а также положений о подразделениях, трудовых договоров, соглашений, подрядов, должностных инструкций и обязанностей руководства, специалистов, рабочих и служащих;
- разработка и осуществление совместно с другими подразделениями мероприятий по обеспечению работы с документами, содержащими конфиденциальные сведения; при всех видах работ организация и контроль выполнения требований «Инструкции по защите конфиденциальной информации»;
- изучение всех сторон производственной, коммерческой, финансовой и другой деятельности для выявления и последующего противодействия любым попыткам нанесения ущерба, ведения учета и анализа нарушений режима безопасности, накопление и анализ данных о злоумышленных устремлениях конкурентной и других организаций, о деятельности предприятия и его клиентов, партнеров, смежников;
- организация и проведение служебных расследований по фактам разглашения сведений, утрат документов, утечки конфиденциальной информации и других нарушений безопасности предприятия;
- разработка, ведение, обновление и пополнение «Перечня сведений конфиденциального характера» и других нормативных актов, регламентирующих

- порядок обеспечения безопасности и защиты информации;
- обеспечение строгого выполнения требований нормативных документов по защите производственных секретов предприятия;
 - осуществление руководства службами и подразделениями безопасности подведомственных предприятий, организаций, учреждений и другими структурами в части оговоренных в договорах условий по защите конфиденциальной информации;
 - организация и регулярное проведение учета сотрудников предприятия и службы безопасности по всем направлениям защиты информации и обеспечения безопасности производственной деятельности;
 - ведение учета и строгого контроля выделенных для конфиденциальной работы помещений, технических средств в них, обладающих потенциальными каналами утечки информации и каналами проникновения к источникам охраняемых секретов;
 - обеспечение проведения всех необходимых мероприятий по пресечению попыток нанесения морального и материального ущерба со стороны внутренних и внешних угроз;
 - поддержание контактов с правоохранительными органами и службами безопасности соседних предприятий в интересах изучения криминогенной обстановки в районе (зоне) и оказания взаимной помощи в кризисных ситуациях.

Служба безопасности является самостоятельной организационной единицей предприятия, подчиняющейся непосредственно руководителю предприятия. Возглавляет службу безопасности начальник службы в должности заместителя руководителя предприятия по безопасности.

Организационно служба безопасности состоит из следующих структурных единиц:

- подразделения режима и охраны;
- специального подразделения обработки документов конфиденциального характера;
- инженерно-технических подразделений;
- информационно-аналитических подразделений.

В таком составе служба безопасности способна обеспечить защиту конфиденциальной информации от любых угроз.

К задачам службы безопасности предприятия относятся:

- определение круга лиц, которые в силу занимаемого служебного положения на предприятии прямо или косвенно имеют доступ к сведениям конфиденциального характера;
- определение участков сосредоточения конфиденциальных сведений;
- определение круга сторонних предприятий, связанных с данным предприятием кооперативными связями, на которых в силу производственных отношений возможен выход из-под контроля сведений конфиденциального характера;
- выявление круга лиц, не допущенных к конфиденциальной информации, но проявляющих повышенный интерес к таким сведениям;
- выявление круга предприятий, в том числе и иностранных, заинтересованных в овладении охраняемыми сведениями с целью нанесения экономического ущерба данному предприятию, устранения экономического конкурента либо его компрометации;
- разработка системы защиты документов, содержащих сведения конфиденциального характера;
- определение на предприятии участков, уязвимых в аварийном отношении, выход из строя которых может нанести материальный ущерб предприятию и сорвать поставки готовой продукции или комплектующих предприятиям, связанным с ним кооперацией;
- определение на предприятии технологического оборудования, выход (или вывод) которого из строя может привести к большим экономическим потерям;
- определение уязвимых мест в технологии производственного цикла, несанкционированное изменение в которой может привести к утрате качества выпускаемой продукции и нанести материальный или моральный ущерб предприятию (потеря конкурентоспособности);
- определение мест на предприятии, несанкционированное посещение которых может привести к изъятию (краже) готовой продукции или полуфабрикатов, заготовок и др. и организация их физической защиты и охраны;

- определение и обоснование мер правовой, организационной и инженерно-технической защиты предприятия, персонала, продукции и информации;
- разработка необходимых мероприятий, направленных на совершенствование системы экономической, социальной и информационной безопасности предприятия;
- внедрение в деятельность предприятия новейших достижений науки и техники, передового опыта в области обеспечения экономической и информационной безопасности;
- организация обучения сотрудников службы безопасности в соответствии с их функциональными обязанностями;
- изучение, анализ и оценка состояния обеспечения экономической и информационной безопасности предприятия и разработка предложений и рекомендаций для их совершенствования;
- разработка технико-экономических обоснований, направленных на приобретение технических средств, получение консультации у специалистов, разработку необходимой документации в целях совершенствования системы мер по обеспечению экономической и информационной безопасности.

Организационные меры являются решающим звеном формирования и реализации комплексной защиты информации и создания системы безопасности предприятия.

2.3. Инженерно техническая защита [^]

На вооружении промышленных шпионов, недобросовестных конкурентов и просто злоумышленников находятся самые разнообразные средства проникновения на объекты противоправных интересов и получения конфиденциальной информации. В этих условиях в интересах обеспечения информационной безопасности необходимы адекватные по ориентации, функциональному назначению и другим характеристикам технические средства защиты охраняемых секретов.

2.3.1. Общие положения [^]

Инженерно-техническая защита (ИТЗ) по определению — это совокупность специальных органов, технических средств и мероприятий по их использованию в интересах защиты конфиденциальной информации.

Многообразие целей, задач, объектов защиты и проводимых мероприятий предполагает рассмотрение некоторой системы классификации средств по виду, ориентации и другим характеристикам.

Например, средства инженерно-технической защиты можно рассматривать по объектам их воздействия. В этом плане они могут применяться для защиты людей, материальных средств, финансов, информации.

Примерная классификационная структура инженерно-технической защиты приведена на рис. 15.

Многообразие классификационных характеристик позволяет рассматривать инженерно-технические средства по объектам воздействия, характеру мероприятий, способам реализации, масштабу охвата, классу средств злоумышленников, которым оказывается противодействие со стороны службы безопасности.

По функциональному назначению средства инженерно-технической защиты делятся на следующие группы:

- физические средства, включающие различные средства и сооружения, препятствующие физическому проникновению (или доступу) злоумышленников на объекты защиты и к материальным носителям конфиденциальной информации (рис. 16) и осуществляющие защиту персонала, материальных средств, финансов и информации от противоправных воздействий;

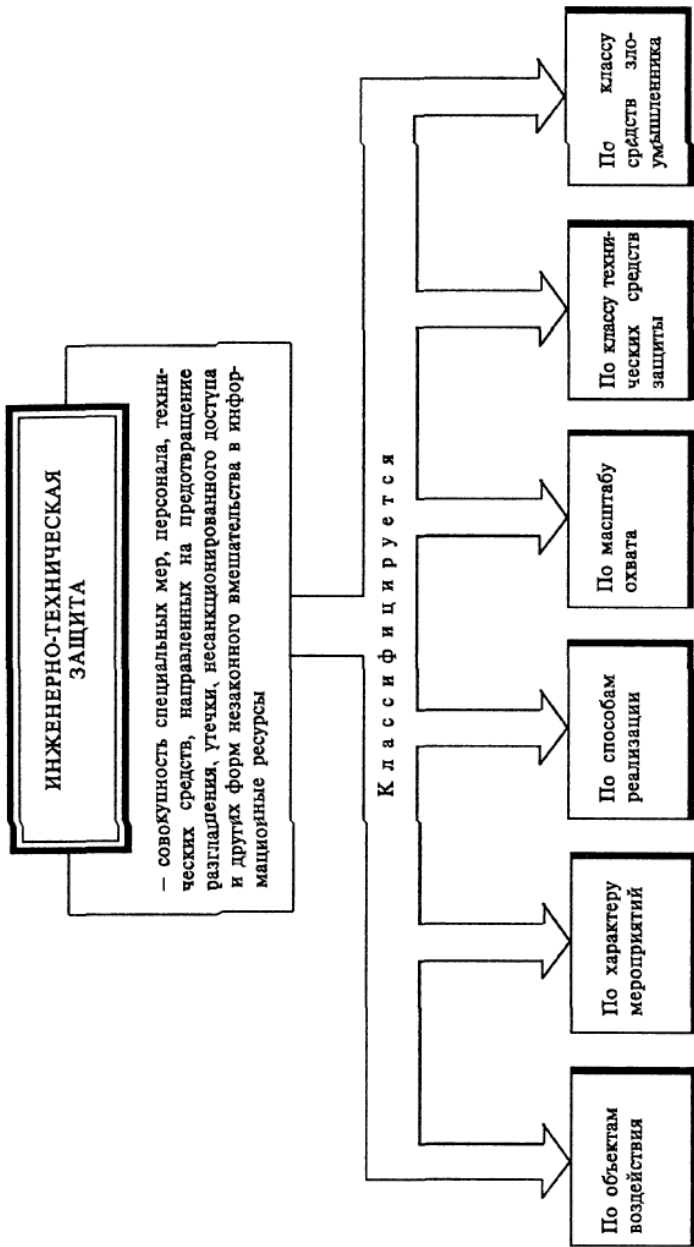


Рис. 15

- аппаратные средства. Сюда входят приборы, устройства, приспособления и другие технические решения, используемые в интересах защиты информации. В практике деятельности предприятия находит широкое применение самая различная аппаратура, начиная с телефонного аппарата до совершенных автоматизированных систем, обеспечивающих производственную деятельность. Основная задача аппаратных средств — обеспечение стойкой защиты информации от разглашения, утечки и несанкционированного доступа через технические средства обеспечения производственной деятельности;
- программные средства, охватывающие специальные программы, программные комплексы и системы защиты информации в информационных системах различного назначения и средствах обработки (сбора, накопления, хранения, обработки и передачи) данных;
- криптографические средства— это специальные математические и алгоритмические средства защиты информации, передаваемой по системам и сетям связи, хранимой и обрабатываемой на ЭВМ с использованием разнообразных методов шифрования.

Аппаратные средства и методы защиты распространены достаточно широко. Однако из-за того, что они не обладают достаточной гибкостью, часто теряют свои защитные свойства при раскрытии их принципов действия и в дальнейшем не могут быть использованы.

Программные средства и методы защиты надежны и период их гарантированного использования без перепрограммирования значительно больше, чем аппаратных.

Криптографические методы занимают важное место и выступают надежным средством обеспечения защиты информации на длительные периоды.

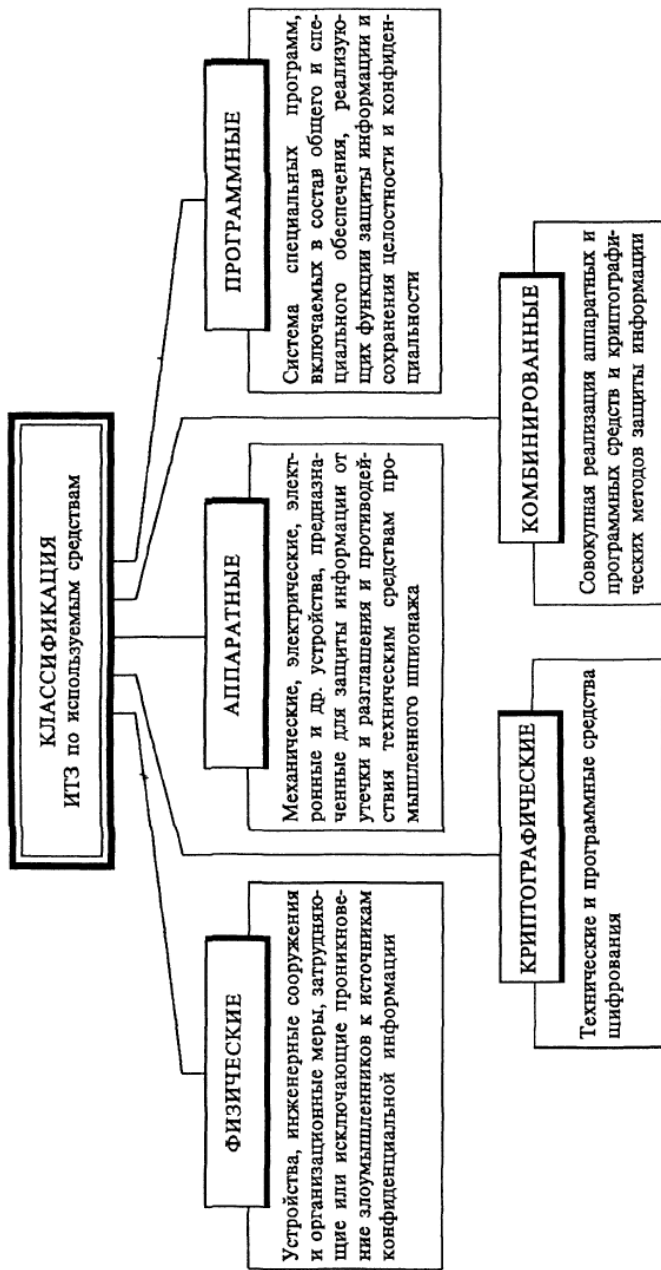


Рис. 16

Очевидно что такое деление средств защиты информации достаточно условно, так как на практике очень часто они: и взаимодействуют и реализуются в комплексе в виде программно-аппаратных модулей с широким использованием алгоритмов закрытия информации.

2.3.2. Физические средства защиты [^]

Физические средства защиты — это разнообразные устройства, приспособления, конструкции, аппараты, изделия, предназначенные для создания препятствий на пути движения злоумышленников.

К физическим средствам относятся механические, электромеханические электронные, электронно-оптические, радио- и радиотехнические и другие устройства для воспрепятствования несанкционированного доступа (входа выхода) проноса (выноса) средств и материалов и других возможных видов преступных действий (рис. 17).

Эти средства применяются для решения следующих задач:

1. охрана территории предприятия и наблюдение за ней;
2. охрана зданий» внутренних помещений и контроль за ними;
3. охрана оборудования, продукции, финансов и информации;
4. осуществление контролируемого доступа в здания и помещения.

Все физические средства защиты объектов можно разделить на три категории: средства предупреждения средства обнаружения и системы ликвидации угроз. Охранив сигнализация и охранное телевидение например, относятся к средствам обнаружения угроз; заборы вокруг объектов — это средства предупреждения несанкционированного проникновения на территорию, а усиленные двери, стены, потолки, решетки на окнах и другие меры служат защитой и от проникновения и от других преступных действий (подслушивание, обстрел, бросание гранат и взрывпакетов и т.д.) Средства пожаротушения относятся к системам ликвидации угроз.

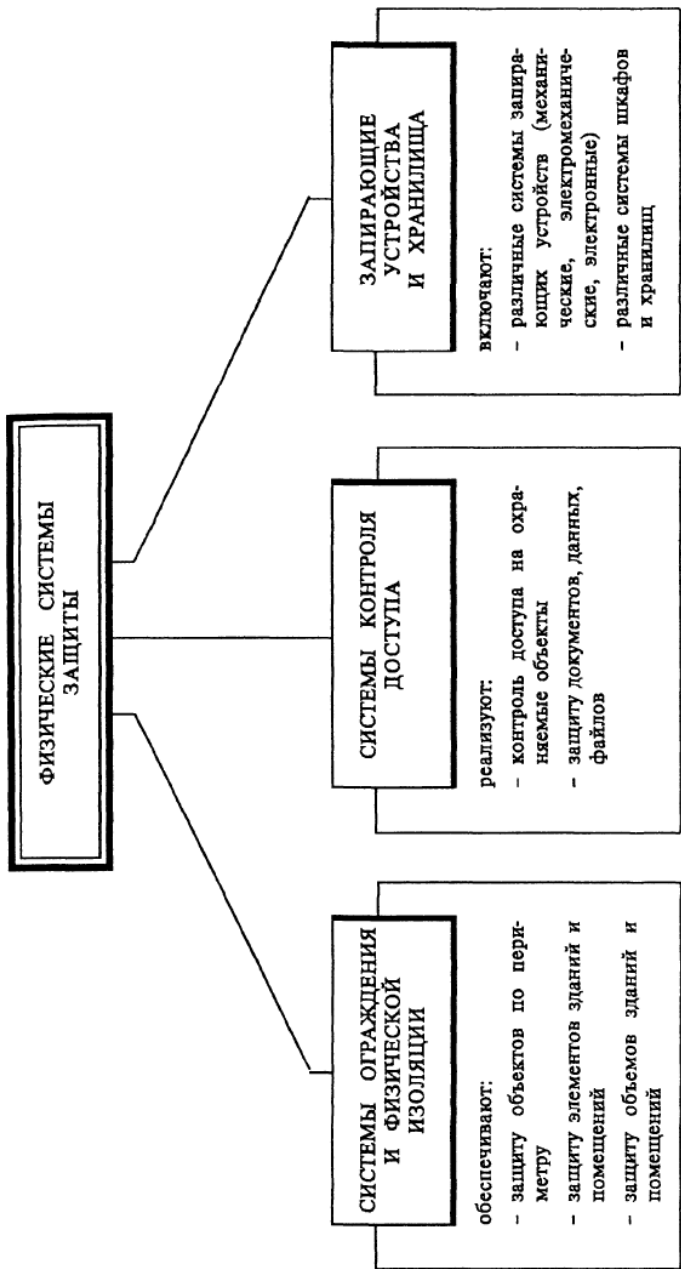


Рис. 17

В общем плане по физической природе и функциональному назначению все средства этой категории можно разделить на следующие группы:

- охранные и охранно-пожарные системы;
- охранные телевидение;
- охранные освещение;
- средства физической защиты.

Охранные системы

Охранные системы и средства охранной сигнализации предназначены для обнаружения различных видов угроз: попыток проникновения на объект защиты, в охраняемые зоны и помещения, попыток проноса (выноса) оружия, средств промышленного шпионажа, краж материальных и финансовых ценностей и других действий; оповещения сотрудников охраны или персонала объекта о появлении угроз и необходимости усиления контроля доступа на объект, территорию, в здания и помещения.

Важнейшими элементами охранных систем являются датчики, обнаруживающие появление угрозы. Характеристики и принципы работы датчиков определяют основные параметры и практические возможности охранных систем.

Уже разработано и широко используется значительное количество самых разнообразных датчиков как по принципам обнаружения различных физических полей, так и по тактическому использованию.

Эффективность работы системы охраны и охранной сигнализации в основном определяется параметрами и принципом работы датчиков. На сегодня известны датчики следующих типов: механические выключатели, проволока с выключателем, магнитный выключатель, ртутный выключатель, коврики давления, металлическая фольга, проволочная сетка, шифроволновый датчик, ультразвуковой датчик, инфракрасный датчик, фотоэлектрический датчик, акустический датчик, вибрационный датчик, индуктивный датчик, емкостный датчик и другие.

Каждый тип датчика реализует определенный вид защиты: точечная защита, защита по линии, защита по площади или защита по объему. Механические датчики ориентированы на защиту линии, коврики давления — на точечное обнаружение, а инфракрасные находят широкое применение по площади и по объему.

Датчики посредством тех или иных каналов связи соединены с контрольно-приемным устройством пункта (или поста) охраны и средствами тревожного оповещения.

Каналами связи в системах охранной сигнализации могут быть специально проложенные проводные или кабельные линии, телефонные линии объекта, линии связи трансляции, системы освещения или радиоканалы. Выбор каналов определяется возможностями объекта.

Важным объектом охранной системы являются средства тревожного оповещения: звонки, лампочки, сирены, подающие постоянные или прерываемые сигналы о появлении угрозы.

По тактическому назначению охранные системы подразделяются на системы охраны:

- периметров объектов;
- помещений и проходов в служебных и складских зданиях;
- сейфов, оборудования, основных и вспомогательных технических средств;
- автотранспорта;
- персонала, в том числе и личного состава охраны, и другие.

К средствам физической защиты относятся:

- естественные и искусственные барьеры;
- особые конструкции периметров, проходов, оконных и дверных переплетов, помещений, сейфов, хранилищ;
- зоны безопасности.

Естественные и искусственные барьеры служат для противодействия незаконному проникновению на территорию объекта. Однако основная защитная нагрузка ложится все-таки на искусственные барьеры — такие, как заборы и другие виды ограждений. Практика показывает, что ограждения сложной конфигурации способны задержать злоумышленника на достаточно большое время. На сегодня насчитывается значительный арсенал таких средств: от простых сетчатых до сложных комбинированных ограждений, оказывающих определенное отпугивающее воздействие на нарушителя.

Особые конструкции периметров, проходов, оконных переплетов, помещений, сейфов, хранилищ являются обязательными с точки зрения безопасности для любых организаций и предприятий. Эти конструкции должны противостоять любым способам физического воздействия со стороны криминальных элементов: механическим деформациям, разрушению сверлением, термическому и механическому резанию,

взрыву; несанкционированному доступу путем подделки ключей, угадывания кода и т. д. Одним из главных технических средств защиты проходов, помещений, сейфов и хранилищ являются замки. Они бывают простыми (с ключами), кодовыми (в том числе и с временной задержкой на открывание) и с программными устройствами, открывающие двери и сейфы только в определенные часы.

Зоны безопасности. Важнейшим средством физической защиты является планировка объекта, его зданий и помещений по зонам безопасности, которые учитывают степень важности различных частей объекта с точки зрения нанесения ущерба от различного вида угроз. Оптимальное расположение зон безопасности и размещение в них эффективных технических средств обнаружения, отражения и ликвидации последствий противоправных действий составляет основу концепции инженерно-технической защиты объекта.

Зоны безопасности должны располагаться на объекте последовательно, от забора вокруг территории объекта до хранилищ ценностей, создавая цепь чередующихся друг за другом препятствий (рубежей), которые придется преодолевать злоумышленнику. Чем сложнее и надежнее препятствие на его пути, тем больше времени потребуется на преодоление каждой зоны и тем больше вероятность того, что расположенные в каждой зоне средства обнаружения (охранные посты, охранная сигнализация и охранное телевидение) выявят наличие нарушителя и подадут сигнал тревоги.

Основу планировки и оборудования зон безопасности объекта составляет принцип равнопрочности границ зон безопасности. Суммарная прочность зон безопасности будет оцениваться наименьшей из них.

Охранное телевидение

Одним из распространенных средств охраны является охранное телевидение. Привлекательной особенностью охранного телевидения является возможность не только отметить нарушение режима охраны объекта, но и контролировать обстановку вокруг него в динамике ее развития, определять опасность действий, вести скрытое наблюдение и производить видеозапись для последующего анализа правонарушения как с целью анализа, так и для привлечения к ответственности нарушителя.

Источниками изображения (датчиками) в системах охранного телевидения являются видеокамеры. Через объектив изображение злоумышленника попадает на светочувствительный элемент камеры, в котором оно преобразуется в электрический сигнал, поступающий затем по специальному коаксиальному кабелю на монитор и при необходимости — на видеомагнитофон.

Видеокамера является наиболее важным элементом системы охранного телевидения, так как от ее характеристик зависит эффективность и результативность всей системы контроля и наблюдения. В настоящее время разработаны и выпускаются самые разнообразные модели, различающиеся как по габаритам, так и по возможностям и по конструктивному исполнению.

Вторым по значимости элементом системы охранного телевидения является монитор. Он должен быть согласован по параметрам с видеокамерой. Часто используется один монитор с несколькими камерами, подсоединяемыми к нему поочередно средствами автоматического переключения по определенному регламенту.

В некоторых системах телевизионного наблюдения предусматривается возможность автоматического подключения камеры, в зоне обзора которой произошло нарушение. Используется и более сложное оборудование, включающее средства автоматизации, — устройства одновременного вывода нескольких изображений, детекторы движения для подачи сигнала тревоги при выявлении каких-либо изменений в изображении.

Охранное освещение

Обязательной составной частью системы защиты любого объекта является охранное освещение. Различают два вида охранного освещения — дежурное и тревожное.

Дежурное освещение предназначается для постоянного использования в нерабочие часы, в вечернее и ночное время как на территории объекта, так и внутри здания.

Тревожное освещение включается при поступлении сигнала тревоги от средства охранной сигнализации. Кроме того, по сигналу тревоги в дополнение к освещению могут включаться и звуковые приборы (звонки, сирены и пр.).

Сигнализация и дежурное освещение должны иметь резервное электропитание на случай аварии или выключения электросети.

Ограждения и физическая изоляция

В последние годы большое внимание уделяется созданию систем физической защиты, совмещенных с системами сигнализации. Так, известна электронная система сигнализации для использования с проволочным ограждением. Система состоит из электронных датчиков и микропроцессора, управляющего блоком обработки данных. Ограждение длиной до 100 м может устанавливаться на открытой местности или размещаться на стенах, чердаках и имеющихся оградах. Устойчивые к воздействию окружающей среды датчики монтируются на стойках, кронштейнах. Проволочное ограждение состоит из 32 горизонтально натянутых стальных нитей, в средней части каждой из которых крепится электромеханический датчик, преобразующий изменение натяжения нитей в электрический сигнал.

Превышение пороговой величины напряжения, программируемое по амплитуде для каждого датчика отдельно, вызывает сигнал тревоги. Связь системы с центральным пунктом управления и контроля осуществляется с помощью мультимплексора. Микропроцессор автоматически через определенные интервалы времени проверяет работу компонентов аппаратуры и программных средств и — в случае установления отклонений — подает соответствующий сигнал.

Подобные и ряд других аналогичных систем физической защиты могут использоваться для защиты объектов по периметру в *целях* обнаружения вторжения на территорию объекта.

Используются системы из сетки двух волоконно-оптических кабелей, по которым передаются кодированные сигналы инфракрасного диапазона. Если в сетке нет повреждений, то сигналы поступают на приемное устройство без искажений. Попытки повреждения сетки приводят к обрывам или деформации кабелей, что вызывает сигнал тревоги. Оптические системы отличаются низким уровнем ложных тревог, вызванных воздействием на нее мелких животных, птиц, изменением погодных условий и высокой вероятностью обнаружения попыток вторжения.

Следующим видом физической защиты является защита элементов зданий и помещений. Хорошую физическую защиту оконных проемов помещений обеспечивают традиционные металлические решетки, а также специальное остекление на основе пластических масс, армированных стальной проволокой. Двери и окна охраняемого помещения оборудуются датчиками,

срабатывающими при разрушении стекол, дверей, но не реагирующими на их колебания, вызванные другими причинами. Срабатывание датчиков вызывает сигнал тревоги.

Среди средств физической защиты особо следует отметить средства защиты ПЭВМ от хищения и проникновения к их внутренним компонентам. Для этого используют металлические конструкции с клейкой подставкой, которая обеспечивает сцепление с поверхностью стола с силой в 2500 — 2700 кг/см. Это исключает изъятие или перемещение ПЭВМ без нарушения целостности поверхности стола. Перемещение ПЭВМ возможно только с использованием специальных ключей и инструментов.

Запирающие устройства

Запирающие устройства и специальные шкафы занимают особое место в системах ограничения доступа, поскольку они несут в себе признаки как систем физической защиты, так и устройств контроля доступа. Они отличаются большим разнообразием и предназначены для защиты документов, материалов, магнитных и фотоносителей и даже технических средств: ПЭВМ, калькуляторов, принтеров, ксероксов и других.

Выпускаются специальные металлические шкафы для хранения ПЭВМ и другой техники. Такие шкафы снабжаются надежной двойной системой запираения: замком ключевого типа и трех — пятизначным комбинированным замком. Фирмы утверждают, что такие шкафы обладают прочностью и надежностью, достаточными для защиты от промышленного шпионажа.

Выпускаются замки с программируемым временем открывания с помощью механических или электронных часов.

Системы контроля доступа

Регулирование доступа в помещения или здания осуществляется прежде всего посредством опознавания службой охраны или техническими средствами.

Контролируемый доступ предполагает ограничение круга лиц, допускаемых в определенные защищаемые зоны, здания, помещения, и контроль за перемещением этих лиц внутри них.

Основанием допуска служит определенный метод опознавания и сравнения с разрешительными параметрами системы. Имеется

весьма широкий спектр методов опознавания уполномоченных лиц на право их доступа в помещения, здания, зоны.

На основе опознавания принимается решение о допуске лиц, имеющих на это право, или запрещение — для не имеющих его. Наибольшее распространение получили атрибутивные и персональные методы опознавания.

К атрибутивным способам относятся средства подтверждения полномочий, такие, в частности, как документы (паспорт, удостоверение), карты (фотокарточки, карты с магнитными, электрическими, механическими идентификаторами и т. д.) и иные средства (ключи, сигнальные элементы и т.д.). Заметим, что эти средства в значительной мере подвержены различного рода подделкам и мошенничеству.

Персональные методы — это методы определения лица по его независимым показателям: отпечаткам пальцев, геометрии рук, особенностям глаз. Персональные характеристики бывают статические и динамические. К последним относятся пульс, давление, кардиограммы, речь, почерк и другие.

Персональные способы наиболее привлекательные. Во-первых, они полно описывают каждого отдельного человека. Во-вторых, невозможно или крайне трудно подделать индивидуальные характеристики.

Статические способы включают анализ физических характеристик — таких, как отпечатки пальцев, особенности геометрии рук и другие. Они достаточно достоверны и обладают малой вероятностью ошибок.

Динамические же способы используют изменяющиеся во времени опознавательные характеристики.

Характеристики, зависящие от привычек и навыков, являются не только наиболее простыми для подделок, но и наиболее дешевыми с точки зрения практической реализации.

Способы опознавания, основанные на чем-либо запоминаемом (код, пароль), могут применяться в случаях наиболее низких требований к безопасности, так как часто эта информация записывается пользователями на различных бумажках, в записных книжках и других носителях, что при их доступности другим может свести на нет все усилия по безопасности. Кроме того, имеется реальная возможность подсмотреть, подслушать или получить эту информацию другим путем (насилие, кража и т. д.).

Способ опознавания человеком (вахтер, часовой) не всегда надежен из-за так называемого «человеческого фактора»,

закрывающегося в том, что человек подвержен влиянию многих внешних условий (усталость, плохое самочувствие, эмоциональный стресс, подкуп). В противовес этому находят широкое применение технические средства опознавания, такие, на пример, как идентификационные карты, опознавание по голосу, почерку, пальцам и др.

Простейший и наиболее распространенный метод идентификации использует различные карты и карточки, на которых помещается кодированная или открытая информация о владельце, его полномочиях и другое.

Обычно это пластиковые карты типа пропусков или жетонов. Карты вводятся в читающее устройство каждый раз, когда требуется войти или выйти из охраняемого помещения или получить доступ к чему-нибудь (сейфу, камере, терминалу).

Существует много разновидностей устройств опознавания и идентификации личности, использующих по добные карты. Одни из них оптическим путем сличают фотографии и другие идентификационные элементы, другие — магнитные поля.

Системы опознавания по отпечаткам пальцев. В основу идентификации положено сравнение относительного положения окончаний и разветвлений линий отпечатка. Поисковая система ищет на текущем изображении контрольные элементы, определенные при исследовании эталонного образца. Для идентификации одного человека считается достаточным определение координат 12 точек.

Эти системы, естественно, весьма сложны и рекомендуются к использованию на объектах, требующих надежной защиты.

Системы опознавания по голосу. Существует несколько способов выделения характерных признаков речи человека: анализ кратковременных сегментов, контрольный анализ, выделение статистических характеристик. Следует отметить, что теоретически вопросы идентификации по голосу разработаны достаточно полно, но промышленное производство пока налажено слабо.

Системы опознавания по почерку считаются наиболее удобными для пользователя. Основным принципом идентификации по почерку является постоянство подписи каждого индивидуума, хотя абсолютного совпадения не бывает.

Система опознавания по геометрии рук. Для идентификации применяют анализ комбинации линий сгибов пальцев и ладони, линий складок, длины и толщины пальцев и других.

Технически это реализуется путем наложения руки на матрицу

фотоячеек. Рука освещается мощной лампой, производится регистрация сигналов с ячеек, не сущих информацию о геометрии.

Все устройства идентификации человека могут работать как отдельно, так и в комплексе. Комплекс может быть узкоспециальным или многоцелевым, при котором система выполняет функции охраны, контроля, регистрации и сигнализации. Такие системы являются уже комплексными. Комплексные системы обеспечивают:

- допуск на территорию предприятия по карточке (пропуску), содержащей индивидуальный машинный код;
- блокирование прохода при попытках несанкционированного прохода (проход без пропуска, проход в спецподразделения сотрудников, не имеющих допуска);
- возможность блокирования прохода для нарушителей графика работы (опоздание, преждевременный уход и т. д.);
- открытие зоны прохода для свободного выхода по команде вахтера;
- проверку кодов пропусков на задержание их предъявителей на КПП по указанию оператора системы;
- регистрацию времени пересечения проходной и сохранение его в базе данных персональной ЭВМ;
- обработку полученных данных и формирование различных документов (табель рабочего времени, суточный рапорт, ведомость нарушителей трудовой дисциплины и т. д.), что позволяет иметь оперативную информацию о нарушителях трудовой дисциплины, отработанном времени;
- оперативную корректировку информации базы данных с доступом по паролю;
- распечатку таблиц рабочего времени по произвольной группе сотрудников (предприятие в целом, структурное подразделение, отдельно выбранные сотрудники);
- распечатку списков нарушителей графика рабочего времени с конкретными данными о нарушении;
- текущий и ретроспективный анализ посещения сотрудниками подразделений, передвижения со сотрудников через КПП, выдачу списочного состава присутствовавших или отсутствовавших в подразделении или на предприятии для произвольно выбранного момента времени (при условии хранения баз данных за прошлые периоды);

- получение оперативной информации абонентами локальной сети в случае сетевой реализации системы.

Физические средства являются первой преградой для злоумышленника при реализации им заходовых методов доступа.

2.3.3. Аппаратные средства защиты [^]

К аппаратным средствам защиты информации относятся самые различные по принципу действия, устройству и возможностям технические конструкции, обеспечивающие пресечение разглашения, защиту от утечки и противодействие несанкционированному доступу к источникам конфиденциальной информации.

Аппаратные средства защиты информации применяются для решения следующих задач:

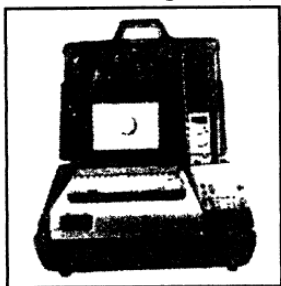
- проведение специальных исследований технических средств обеспечения производственной деятельности на наличие возможных каналов утечки информации;
- выявление каналов утечки информации на разных объектах и в помещениях;
- локализация каналов утечки информации;
- поиск и обнаружение средств промышленного шпионажа;
- противодействие несанкционированному доступу к источникам конфиденциальной информации и другим действиям.

По функциональному назначению аппаратные средства могут быть классифицированы на средства обнаружения, средства поиска и детальных измерений, средства активного и пассивного противодействия. При этом по своим техническим возможностям средства защиты информации могут быть общего назначения, рассчитанные на использование непрофессионалами с целью получения предварительных (общих) оценок, и профессиональные комплексы, позволяющие проводить тщательный поиск, обнаружение и прецизионные измерения все характеристик средств промышленного шпионажа. В качестве примера первых можно рассмотреть группу индикаторов электромагнитных излучений типа ИП, обладающих широким спектром принимаемых сигналов и довольно низкой чувствительностью. В качестве второго примера

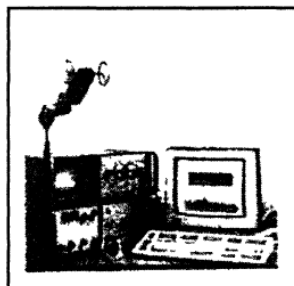
— комплекс для обнаружения и пеленгования радиозакладок, предназначенный для автоматического обнаружения и определения местонахождения радиопередатчиков, радиомикрофонов, телефонных закладок и сетевых радиопередатчиков. Это уже сложный современный поисково-обнаружительный профессиональный комплекс. Таким является, например, комплекс «Дельта», который обеспечивает:

- достоверное обнаружение практически любых из имеющихся в продаже радиомикрофонов, радиостетоскопов, сетевых и телефонных передатчиков, в том числе и с инверсией спектра;
- автоматическое определение места расположения микрофонов в объеме контролируемого помещения.

В состав комплекса входит радиоприемное устройство AR-3000 и ПЭВМ (рис. 18).



*Рис. 18.
Разведывательно-
поисковый комплекс
«Дельта»*



*Рис. 19. Комплекс
обнаружения и измерения
ПЭМИ «Зарница»*

Поисковую аппаратуру можно подразделить на аппаратуру поиска средств съема информации и исследования: каналов ее утечки.

Аппаратура первого типа направлена на поиск и локализацию уже внедренных злоумышленниками средств несанкционированного доступа. Аппаратура второго типа предназначена для выявления каналов утечки информации.

Примером такого комплекса может служить комплекс «Зарница», обеспечивающий измерение параметров побочных электромагнитных излучений в диапазоне частот от 10 КГц до 1 ГГц. Обработка результатов измерений осуществляется на ПЭВМ в

соответствии с действующими нормативно-методическими Документами Гостехкомиссии при Президенте РФ (рис. 19).

Определяющими для такого рода систем являются оперативность исследования и надежность полученных результатов.

Использование профессиональной поисковой аппаратуры требует высокой квалификации оператора. Как в любой области техники, универсальность той или иной аппаратуры приводит к снижению ее параметров по каждой отдельной характеристике.

С другой стороны, существует огромное количество различных по физической природе каналов утечки информации, а также физических принципов, на основе которых работают системы несанкционированного доступа. Эти факторы обуславливают многообразие поисковой аппаратуры, а ее сложность определяет высокую стоимость каждого прибора. В связи с этим достаточный комплекс поискового оборудования могут позволить себе иметь структуры, постоянно проводящие соответствующие обследования. Это либо крупные службы безопасности, либо специализированные фирмы, оказывающие услуги сторонним организациям.

Конечно, описанное выше не является аргументом для отказа от использования средств поиска самостоятельно. Но эти средства в большинстве случаев достаточно просты и позволяют проводить профилактические мероприятия в промежутке между серьезными поисковыми обследованиями.

В особую группу выделяются аппаратные средства защиты ЭВМ и коммуникационных систем на их базе.

Аппаратные средства защиты применяются как в отдельных ПЭВМ, так и на различных уровнях и участках сети: в центральных процессорах ЭВМ, в их оперативных ЗУ (ОЗУ), контроллерах ввода-вывода, внешних ЗУ, терминалах и т. д.

Для защиты центральных процессоров (ЦП) применяется кодовое резервирование — создание дополнительных битов в форматах машинных команд (разрядов секретности) и резервных регистров (в устройствах ЦП). Одновременно предусматриваются два возможных режима работы процессора, которые отделяют вспомогательные операции от операций непосредственного решения задач пользователя. Для этого служит специальная система прерывания, реализуемая аппаратными средствами.

Одной из мер аппаратной защиты ЭВМ и информационных сетей является ограничение доступа к оперативной памяти с

помощью установления границ или полей. Для этого создаются регистры контроля и регистры защиты данных. Применяются также дополнительные биты четности — разновидность метода кодового резервирования.

Для обозначения степени конфиденциальности программ и данных, категорий пользователей используются биты, называемые битами конфиденциальности (это два-три дополнительных разряда, с помощью которых кодируются категории секретности пользователей, программ и данных).

Программы и данные, загружаемые в ОЗУ, нуждаются в защите, гарантирующей их от несанкционированного доступа. Часто используются биты четности, ключи, постоянная специальная память. При считывании из ОЗУ необходимо, чтобы программы не могли быть уничтожены несанкционированными действиями пользователей или вследствие выхода аппаратуры из строя. Отказы должны своевременно выявляться и устраняться, чтобы предотвратить исполнение искаженной команды ЦП и потери информации.

Для предотвращения считывания оставшихся после обработки данных в ОЗУ применяется специальная схема стирания. В этом случае формируется команда на стирание ОЗУ и указывается адрес блока памяти, который должен быть освобожден от информации. Эта схема записывает нули или какую-нибудь другую последовательность символов во все ячейки данного блока памяти, обеспечивая надежное стирание ранее загруженных данных.

Аппаратные средства защиты применяются и в терминалах пользователей. Для предотвращения утечки информации при подключении незарегистрированного терминала необходимо перед выдачей запрашиваемых данных осуществить идентификацию (автоматическое определение кода или номера) терминала, с которого поступил запрос. В многопользовательском режиме этого терминала идентификация его недостаточна. Необходимо осуществить аутентификацию пользователя, то есть установить его подлинность и полномочия. Это необходимо и потому, что разные пользователи, зарегистрированные в системе, могут иметь доступ только к отдельным файлам и строго ограниченные полномочия их использования.

Для идентификации терминала чаще всего применяется генератор кода, включенный в аппаратуру терминала, а для аутентификации пользователя — такие аппаратные средства, как ключи, персональные кодовые карты, персональный

идентификатор, устройства распознавания голоса пользователя или формы его пальцев. Но наиболее распространенными средствами аутентификации являются пароли, проверяемые не аппаратными, а программными средствами опознавания.

Аппаратные средства защиты информации — это различные технические устройства, системы и сооружения, предназначенные для защиты информации от разглашения, утечки и несанкционированного доступа.

2.3.4. Программные средства защиты [^]

Системы защиты компьютера от чужого вторжения весьма разнообразны и классифицируются, как:

- средства собственной защиты, предусмотренные общим программным обеспечением;
- средства защиты в составе вычислительной системы;
- средства защиты с запросом информации;
- средства активной защиты;
- средства пассивной защиты и другие.

Более подробно эти группы защиты представлены на рис. 20.

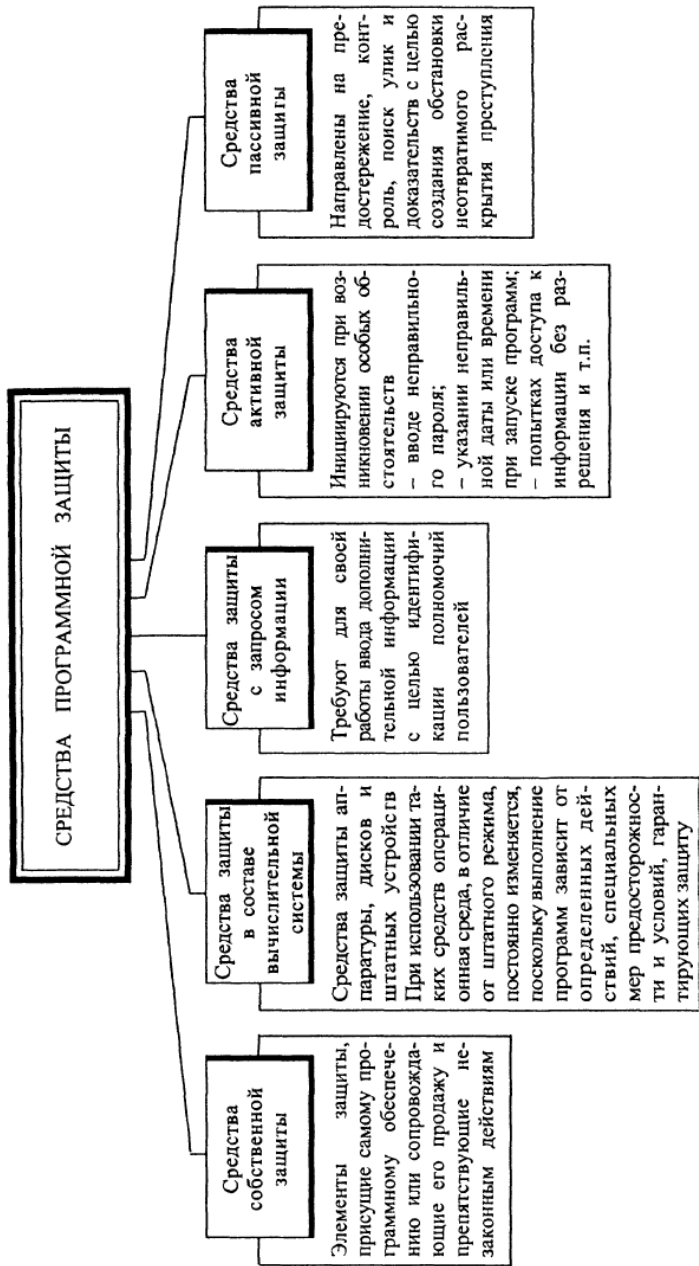


Рис. 20

Основные направления использования программной защиты информации

Можно выделить следующие направления использования программ для обеспечения безопасности конфиденциальной информации, в частности такие:

- защита информации от несанкционированного доступа;
- защита информации от копирования;
- защита программ от копирования;
- защита программ от вирусов;
- защита информации от вирусов;
- программная защита каналов связи.

По каждому из указанных направлений имеется достаточное количество качественных, разработанных профессиональными организациями и распространяемых на рынках программных продуктов (рис. 21).

Программные средства защиты имеют следующие разновидности специальных программ:

- идентификации технических средств, файлов и аутентификации пользователей;
- регистрации и контроля работы технических средств и пользователей;
- обслуживания режимов обработки информации ограниченного пользования;
- защиты операционных средств ЭВМ и прикладных программ пользователей;
- уничтожения информации в защитные устройства после использования;
- сигнализирующих нарушения использования ресурсов;
- вспомогательных программ защиты различного назначения (рис. 22).

Идентификация технических средств и файлов, осуществляемая программно, делается на основе анализа регистрационных номеров различных компонентов и объектов информационной системы и сопоставления их со значениями адресов и паролей, хранящихся в защитном устройстве системы управления.

Для обеспечения надежности защиты с помощью паролей работа системы защиты организуется таким образом, чтобы вероятность раскрытия секретного

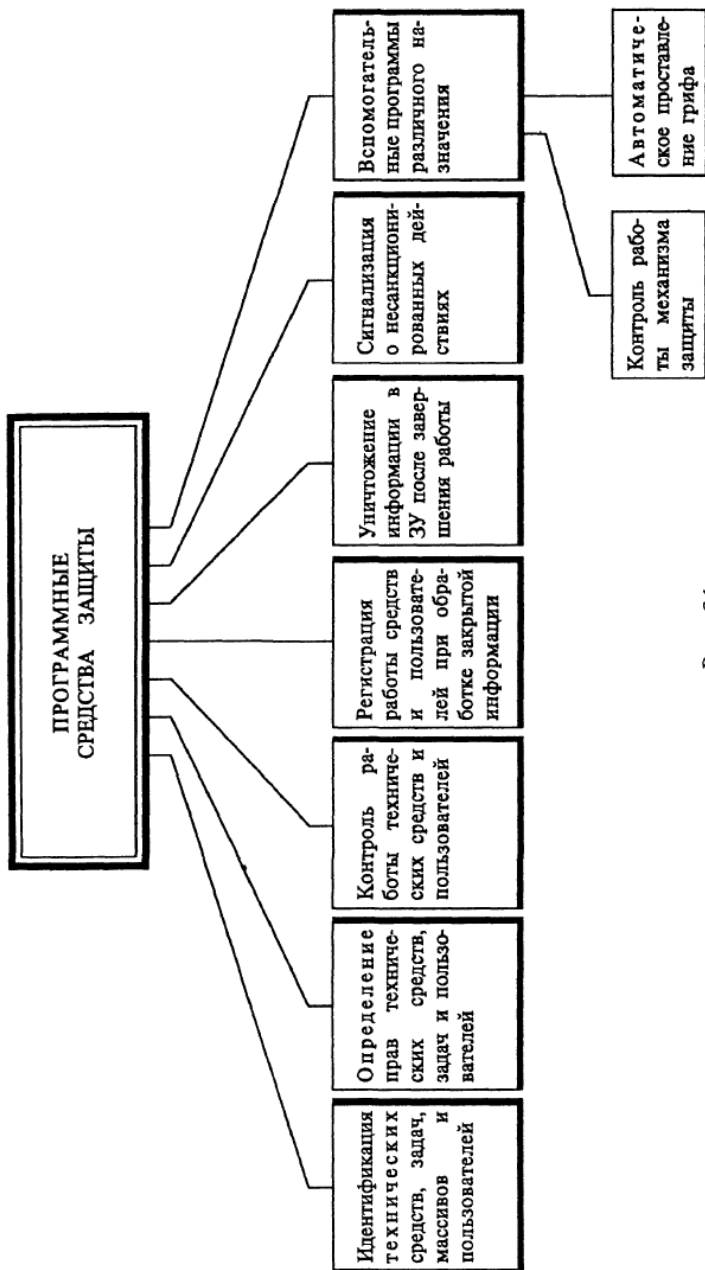


Рис. 21

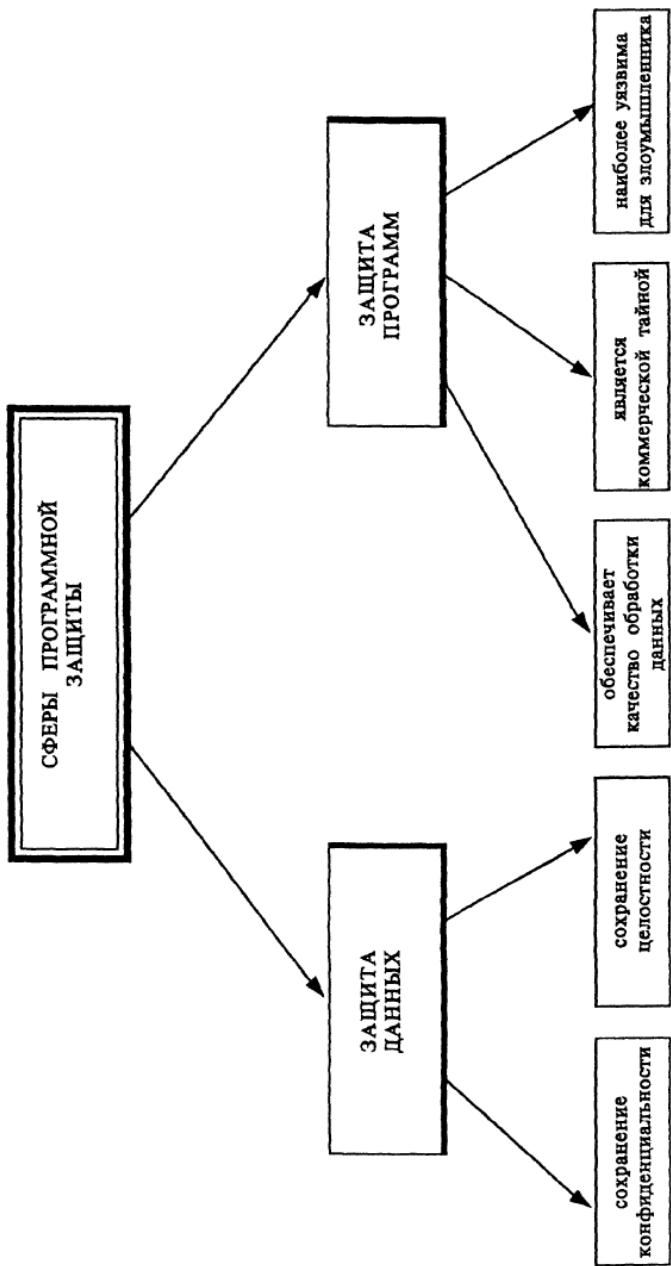


Рис. 22

пароля и установления соответствия тому или иному идентификатору файла или терминала была как можно меньше. Для этого надо периодически менять пароль, а число символов в нем установить достаточно большим.

Эффективным способом идентификации адресуемых элементов и аутентификации пользователей является алгоритм запросно-ответного типа, в соответствии с которым система защиты выдает пользователю запрос на пароль, после чего он должен дать на него определенный ответ. Так как моменты ввода запроса и ответа на него непредсказуемы, это затрудняет процесс отгадывания пароля, обеспечивая тем самым более высокую надежность защиты.

Получение разрешения на доступ к тем или иным ресурсам можно осуществить не только на основе использования секретного пароля и последующих процедур аутентификации и идентификации. Это можно сделать более детальным способом, учитывающим различные особенности режимов работы пользователей, их полномочия, категории запрашиваемых данных и ресурсов. Этот способ реализуется специальными программами, анализирующими соответствующие характеристики пользователей, содержание заданий, параметры технических и программных средств, устройств памяти.

Поступающие в систему защиты конкретные данные, относящиеся к запросу, сравниваются в процессе работы программ защиты с данными, занесенными в регистрационные секретные таблицы (матрицы). Эти таблицы, а также программы их формирования и обработки хранятся в зашифрованном виде и находятся под особым контролем администратора (администраторов) безопасности информационной сети.

Для разграничения обращения отдельных пользователей к вполне определенной категории информации применяются индивидуальные меры секретности этих файлов и особый контроль доступа к ним пользователей. Гриф секретности может формироваться в виде трехрядных кодовых слов, которые хранятся в самом файле или в специальной таблице. В этой же таблице записываются идентификатор пользователя, создавшего данный файл, идентификаторы терминалов, с которых может быть осуществлен доступ к файлу, идентификаторы пользователей, которым разрешен доступ к данному файлу, а также их права на пользование файлом (считывание, редактирование, стирание, обновление, исполнение и т. д.). Важно не допустить

взаимовлияния пользователей в процессе обращения к файлам. Если, например, одну и ту же запись имеют право редактировать несколько пользователей, то каждому из них необходимо сохранить именно его вариант редакции (делается несколько копий записей с целью возможного анализа и установления полномочий).

Защита информации от несанкционированного доступа

Для защиты от чужого вторжения обязательно предусматриваются определенные меры безопасности. Основные функции, которые должны осуществляться программными средствами, это:

- идентификация субъектов и объектов;
- разграничение (иногда и полная изоляция) доступа к вычислительным ресурсам и информации;
- контроль и регистрация действий с информацией и программами.

Процедура идентификации и подтверждения подлинности предполагает проверку, является ли субъект, осуществляющий доступ (или объект, к которому осуществляется доступ), тем, за кого себя выдает. Подобные проверки могут быть одноразовыми или периодическими (особенно в случаях продолжительных сеансов работы). В процедурах идентификации используются различные методы.

- простые, сложные или одноразовые пароли;
- обмен вопросами и ответами с администратором;
- ключи, магнитные карты, значки, жетоны;
- средства анализа индивидуальных характеристик (голоса, отпечатков пальцев, геометрических параметров рук, лица);
- специальные идентификаторы или контрольные суммы для аппаратуры, программ, данных.

Наиболее распространенным методом идентификации является парольная идентификация.

Практика показала, что парольная защита данных является слабым звеном, так как пароль можно подслушать или подсмотреть, пароль можно перехватить, а то и просто разгадать.

Для защиты самого пароля выработаны определенные рекомендации, как сделать пароль надежным:

- пароль должен содержать по крайней мере восемь символов. Чем меньше символов содержит пароль, тем

- легче его разгадать;
- не используйте в качестве пароля очевидный набор символов, например ваше имя, дату рождения, имена близких или наименования ваших программ. Лучше всего использовать для этих целей неизвестную формулу или цитату;
- если криптографическая программа позволяет, введите в пароль по крайней мере один пробел, небуквенный символ или прописную букву; не называйте никому ваш пароль, не записывайте его. Если вам пришлось нарушить эти правила, спрячьте листок в запираемый ящик;
- чаще меняйте пароль,
- не вводите пароль в процедуру установления диалога или макрокоманду.

Помните, что набранный на клавиатуре пароль часто сохраняется в последовательности команд автоматического входа в систему.

Для идентификации программ и данных часто прибегают к подсчету контрольных сумм, однако, как и в случае парольной идентификации, важно исключить возможность подделки при сохранении правильной контрольной суммы. Это достигается путем использования сложных методов контрольного суммирования на основе криптографических алгоритмов. Обеспечить защиту данных от подделки (имитостойкость) можно, применяя различные методы шифрования и методы цифровой подписи на основе криптографических систем с открытым ключом.

После выполнения процедур идентификации и установления подлинности пользователь получает доступ к вычислительной системе, и защита информации осуществляется на трех уровнях:

- аппаратуры;
- программного обеспечения;
- данных.

Защита на уровне аппаратуры и программного обеспечения предусматривает управление доступом к вычислительным ресурсам: отдельным устройствам, оперативной памяти, операционной системе, специальным служебным или личным программам пользователя.

Защита информации на уровне данных направлена:

- на защиту информации при обращении к ней в процессе работы на ПЭВМ и выполнении только

- разрешенных операций над ними;
- на защиту информации при ее передаче по каналам связи между различными ЭВМ.

Управление доступом к информации позволяет ответить на вопросы:

- кто может выполнять и какие операции;
- над какими данными разрешается выполнять операции.

Объектом, доступ к которому контролируется, может быть файл, запись в файле или отдельное поле записи файла, а в качестве факторов, определяющих порядок доступа, — определенное событие, значения данных, состояние системы, полномочия пользователя, предыстория обращения и другие данные.

Доступ, управляемый событием, предусматривает блокировку обращения пользователя. Например, в определенные интервалы времени или при обращении с определенного терминала. Доступ, зависящий от состояния, осуществляется в зависимости от текущего состояния вычислительной системы, управляющих программ и системы защиты.

Что касается доступа, зависящего от полномочий, то он предусматривает обращение пользователя к программам, данным, оборудованию в зависимости от предоставленного режима. Такими режимами могут быть «только читать», «читать и писать», «только выполнять» и другие.

В основе большинства средств контроля доступа лежит то или иное представление матрицы доступа.

Другой подход к построению средств защиты доступа основан на контроле информационных потоков и разделении субъектов и объектов доступа на классы конфиденциальности.

Средства регистрации, как и средства контроля доступа, относятся к эффективным мерам защиты от несанкционированных действий. Однако, если средства контроля доступа предназначены для предотвращения таких действий, то задача регистрации — обнаружить уже совершенные действия или их попытки.

В общем комплекс программно-технических средств и организованных (процедурных) решений по защите информации от несанкционированного доступа (НСД) реализуется следующими действиями:

- управлением доступом;
- регистрацией и учетом;
- применением криптографических средств;

- обеспечением целостности информации.

Можно отметить следующие формы контроля и разграничения доступа, нашедшие широкое применение на практике:

1. Предотвращение доступа:
 - a. к жесткому диску;
 - b. к отдельным разделам;
 - c. к отдельным файлам;
 - d. к каталогам;
 - e. к гибким дискам;
 - f. к сменным носителям информации.
2. Установка привилегий доступа к группе файлов.
3. Защита от модификации:
 - a. файлов;
 - b. каталогов.
4. Защита от уничтожения:
 - a. файлов;
 - b. каталогов.
5. Предотвращение копирования:
 - a. файлов;
 - b. каталогов;
 - c. прикладных программ.
6. Затемнение экрана по истечении времени, установленного пользователем.

В обобщенном виде средства защиты данных приведены на рис. 23.

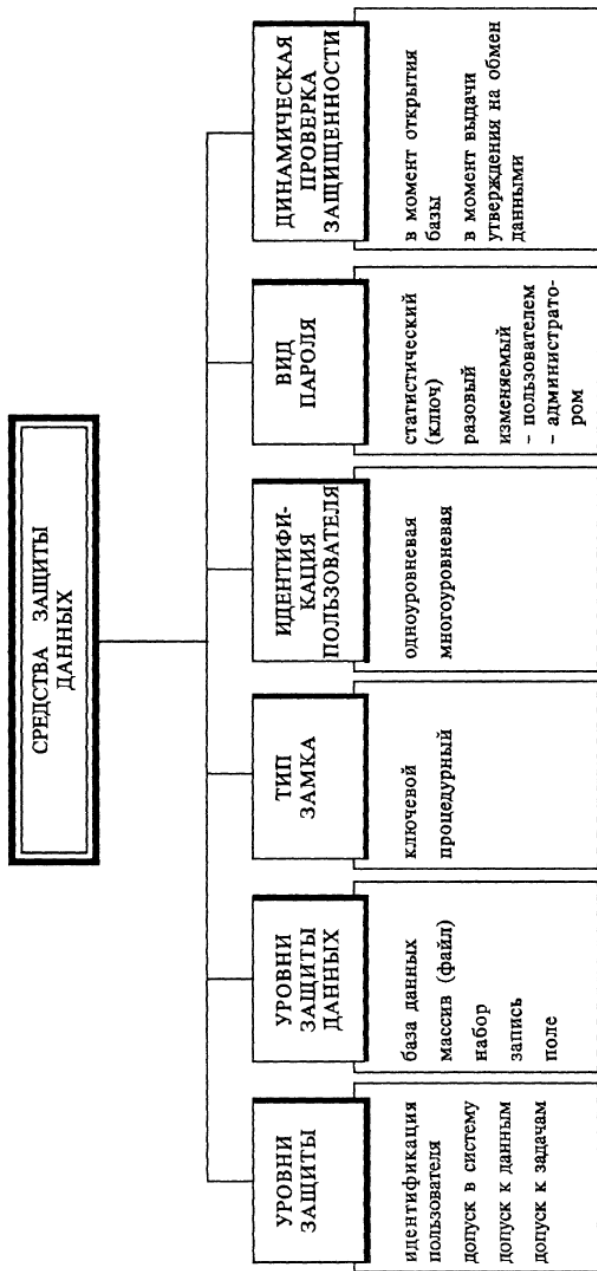


Рис. 23

Защита от копирования

Средства защиты от копирования предотвращают использование ворованных копий программного обеспечения и являются в настоящее время единственно надежным средством — как защищающим авторское право программистов-разработчиков, так и стимулирующим развитие рынка. Под средствами защиты от копирования понимаются средства, обеспечивающие выполнение программой своих функций только при опознании некоторого уникального не копируемого элемента. Таким элементом (называемым ключевым) может быть дискета, определенная часть компьютера или специальное устройство, подключаемое к ПЭВМ. Защита от копирования реализуется выполнением ряда функций, являющихся общими для всех систем защиты:

- идентификация среды, из которой будет запускаться программа;
- аутентификация среды, из которой запущена программа;
- реакция на запуск из несанкционированной среды;
- регистрация санкционированного копирования;
- противодействие изучению алгоритмов работы системы.

Под средой, из которой будет запускаться программа, подразумевается либо дискета, либо ПЭВМ (если установка происходит на НЖМД). Идентификация среды заключается в том, чтобы некоторым образом поименовать среду с целью дальнейшей ее аутентификации. Идентифицировать среду — значит закрепить за ней некоторые специально созданные или измеренные редко повторяющиеся и трудно подделываемые характеристики — идентификаторы. Идентификация дискет может быть проведена двумя способами.

Первый основан на нанесении повреждений на некоторую часть поверхности дискеты. Распространенный способ такой идентификации — «лазерная дыра». При таком способе дискета прожигается в некотором месте лазерным лучом. Очевидно, что сделать «» точно такую же дырку в дискете-копии и в том же самом месте, как и на дискете-оригинале, достаточно сложно.

Второй способ идентификации основан на нестандартном форматировании дискеты.

Реакция на запуск из несанкционированной среды обычно сводится к выдаче соответствующего сообщения.

Защита информации от разрушения

Одной из задач обеспечения безопасности для всех случаев пользования ПЭВМ является защита информации от разрушения, которое может произойти при подготовке и осуществлении различных восстановительных мероприятий (резервировании, создании и обновлении страховочного фонда, ведении архивов информации и других). Так как причины разрушения информации весьма разнообразны (несанкционированные действия, ошибки программ и оборудования, компьютерные вирусы и пр.), то проведение страховочных мероприятий обязательно для всех, кто пользуется персональными ЭВМ.

Необходимо специально отметить опасность компьютерных вирусов. Многие пользователи ЭВМ (ПЭВМ) о них хорошо знают, а тот, кто с ними еще не знаком, скоро познакомится. Вирус компьютерный — небольшая, достаточно сложная, тщательно составленная и опасная программа, которая может самостоятельно размножаться, переносить себя на диски, прикрепляться к чужим программам и передаваться по информационным сетям. Вирус обычно создается для нарушения работы компьютера различными способами — от «безобидной» выдачи какого-либо сообщения до стирания, разрушения файлов. Основную массу вирусов создают люди, хулиганствующие программисты, в основном, чтобы потешить свое самолюбие или заработать деньги на продаже антивирусов. Антивирус — программа, обнаруживающая или обнаруживающая и удаляющая вирусы. Такие программы бывают специализированными и универсальными. Чем отличается универсальный антивирус от специализированного? Специализированный способен бороться только с уже написанными, работающими вирусами, а универсальный — и с еще не написанными.

К специализированным относится большинство антивирусных программ: AIDSTEST, VDEATH, SERUM-3, ANTI-KOT, SCAN и сотни других. Каждая из них распознает один или несколько конкретных вирусов, никак не реагируя на присутствие остальных.

Универсальные антивирусы предназначены для борьбы с целыми классами вирусов. По назначению антивирусы универсального действия бывают довольно различны. Широкое применение находят резидентные антивирусы и программы-ревизоры.

И те и другие антивирусные программы обладают определенными возможностями, положительными и отрицательными (недостатки) характеристиками. Специализированные при своей простоте слишком узко специализированы. При значительном разнообразии вирусов требуется такое же многообразие антивирусов.

Помимо использования в интересах защиты от вирусов антивирусных программ широко используют и организационные меры безопасности. Для уменьшения опасности вирусных актов возможно предпринять определенные действия, которые для каждого конкретного случая могут быть сокращены или расширены. Вот некоторые из таких действий:

1. Информировать всех сотрудников предприятия об опасности и возможном ущербе в случае вирусных атак.
2. Не осуществлять официальные связи с другими предприятиями по обмену (получению) программным обеспечением. Запретить сотрудникам приносить программы «со стороны» для установки их в системы обработки информации. Должны использоваться только официально распространяемые программы.
3. Запретить сотрудникам использовать компьютерные игры на ПЭВМ, обрабатывающих конфиденциальную информацию.
4. Для выхода на сторонние информационные сети выделить отдельное специальное место.
5. Создать архив копий программ и данных.
6. Периодически проводить проверку контрольным суммированием или сравнением с «чистыми» программами.
7. Установить системы защиты информации на особо важных ПЭВМ. Применять специальные антивирусные средства.

Программная защита информации — это система специальных программ, включаемых в состав программного обеспечения, реализующих функции защиты информации.

2.3.5. Криптографические средства защиты [^]

Криптография как средство защиты (закрытия) информации приобретает все более важное значение в мире коммерческой

деятельности.

Криптография имеет достаточно давнюю историю. Вначале она применялась главным образом в области военной и дипломатической связи. Теперь она необходима в производственной и коммерческой деятельности. Если учесть, что сегодня по каналам шифрованной связи только у нас в стране передаются сотни миллионов сообщений, телефонных переговоров, огромные объемы компьютерных и телеметрических данных, и все это, что называется, не для чужих глаз и ушей, становится ясным: сохранение тайны этой переписки крайне необходимо.

Что же такое криптография? Она включает в себя несколько разделов современной математики, а также специальные отрасли физики, радиоэлектроники, связи и *некоторых других смежных отраслей*. (Ее задачей является преобразование математическими методами передаваемого по каналам связи секретного сообщения, телефонного разговора или компьютерных данных таким образом, что они становятся совершенно непонятными для посторонних лиц. То есть криптография должна обеспечить такую защиту секретной (или любой другой) информации, что даже в случае ее перехвата посторонними лицами и обработки любыми способами с использованием самых быстродействующих ЭВМ и последних достижений науки и техники, она не должна быть дешифрована в течение нескольких десятков лет. Для такого преобразования информации используются различные шифровальные средства — такие, как средства шифрования документов, в том числе и портативного исполнения, средства шифрования речи (телефонных и радиопереговоров), средства шифрования телеграфных сообщений и передачи данных.

Общая технология шифрования

Исходная информация, которая передается по каналам связи, может представлять собой речь, данные, видеосигналы, называется незашифрованными сообщениями P (рис. 24).

В устройстве шифрования сообщение P шифруется (преобразуется в сообщение C) и передается по «незакрытому» каналу связи. На приемной стороне сообщение C дешифруется для восстановления исходного значения сообщения P .

Параметр, который может быть применен для извлечения отдельной информации, называется ключом.

В современной криптографии рассматриваются два типа

криптографических алгоритмов (ключей). Это классические криптографические алгоритмы, основанные на использовании секретных ключей, и новые криптографические алгоритмы с открытым ключом, основанные на использовании ключей двух типов: секретного (закрытого) и открытого.

В криптографии с открытым ключом имеются по крайней мере два ключа, один из которых невозможно вычислить из другого. Если ключ расшифрования вычислительными методами невозможно получить из ключа зашифрования, то секретность информации, зашифрованной с помощью несекретного (открытого) ключа, будет обеспечена. Однако этот ключ должен быть защищен от подмены или модификации. Ключ расшифрования также должен быть секретным и защищен от подмены или модификации.

Если, наоборот, вычислительными методами невозможно получить ключ зашифрования из ключа расшифрования, то ключ расшифрования может быть не секретным.

Разделение функций зашифрования и расшифрования посредством разделения на две части дополнительной информации, требуемой для выполнения операций, является той ценной идеей, которая лежит в основе криптографии с открытым ключом.

МОДЕЛЬ КРИПТОГРАФИЧЕСКОЙ СИСТЕМЫ

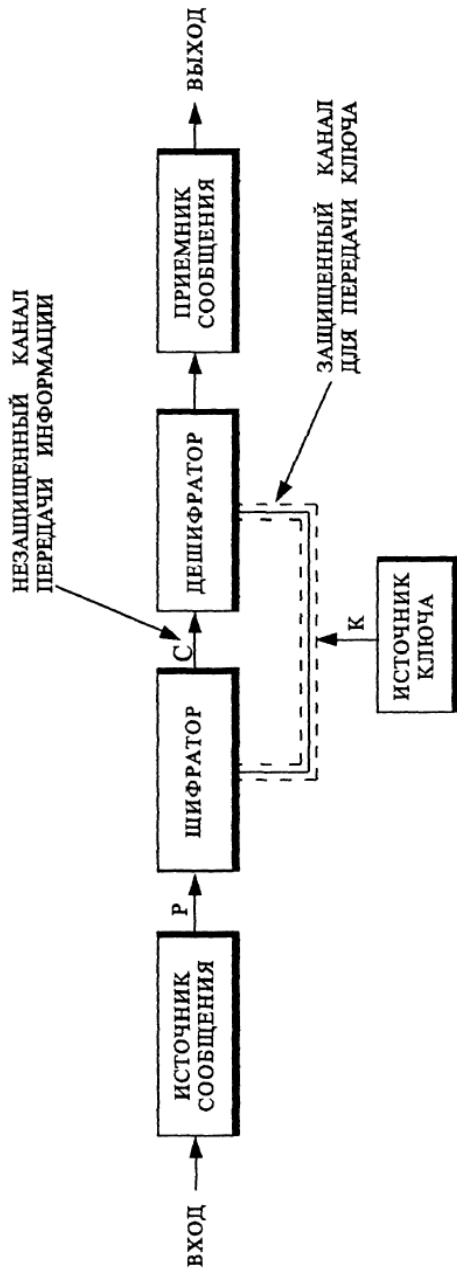


Рис. 24

Технология шифрования речи

Наиболее распространенным способом шифрования аналогового речевого сигнала является разделение его на части.

В этом случае входной речевой сигнал поступает в полосовые фильтры для выделения полос шифруемого спектра. Выходной сигнал каждого фильтра в процессе шифрования подвергается либо перестановке по частоте, либо перевертыванию спектра (инверсия), либо и тому и другому одновременно. Затем синтезируется полный шифровальный выходной сигнал.

По этому принципу работает система AVPS (Analog Voice Privided System) — речевой шифратор (скремблер), который осуществляет перестановку отдельных «вырезов» входного сигнала с помощью полосового фильтра — анализатора. Система имеет 12 ключей шифрования, обусловленных возможными перестановками, что обеспечивает надежность используемого метода.

Система AVPS используется в реальном времени с любыми унифицированными телефонами. Качество шифрования речи высокое, сохраняется узнаваемость абонента.

Находят очень широкое распространение цифровые системы шифрования речевых сигналов. Эти системы обеспечивают высокую надежность шифрования.

В системах шифрования данных используются в основном две элементарные системы:

1. Перестановка (биты или подблоки внутри каждого блока входных данных переставляются).
2. Замещение (биты или подблоки внутри каждого блока входных данных заменяются).

Разработано большое число алгоритмов шифрования. К числу наиболее эффективных относится алгоритм DES (Data Encryption Standart) — стандарт шифрования данных. Американское национальное бюро по стандартизации NBS узаконило алгоритм DES в качестве стандарта для систем связи. Механизм шифрования в этом алгоритме основывается на использовании ключа длиной 56 бит.

Для защиты промышленной и коммерческой информации на международном и отечественном рынках предлагаются различные технические устройства и комплекты профессиональной аппаратуры шифрования и криптозащиты телефонных и радиопереговоров, деловой переписки и пр.

Широкое распространение получили скремблеры и

маскираторы, заменяющие речевой сигнал цифровой передачей данных. Производятся средства защиты телетайпов, телексов и факсов. Для этих целей используются шифраторы, выполняемые в виде отдельных устройств, в виде приставок к аппаратам или встраиваемые в конструкцию телефонов, факс-модемов и других аппаратов связи (радиостанции и другие).

Распространенность шифрования как средства обеспечения безопасности теми или иными средствами можно характеризовать следующими данными (рис.25).

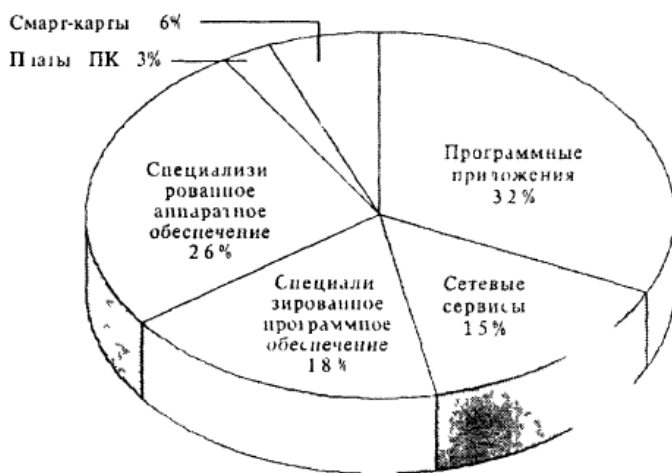


Рис. 25

Аппаратные, программные, программно-аппаратные и криптографические средства реализуют те или иные услуги информационной безопасности различными механизмами защиты информации, обеспечивающими соблюдение конфиденциальности, целостности, полноты и доступности.

Инженерно-техническая защита информации использует физические, аппаратные, программные и криптографические средств.

Выводы

1. Комплексная безопасность информационных ресурсов достигается использованием правовых актов государственного и ведомственного уровня, организационных мер и технических средств защиты информации от различных внутренних и внешних угроз.
2. Правовые меры обеспечения безопасности и защиты информации являются основой порядка деятельности и поведения сотрудников всех уровней и степени их ответственности за нарушения установленных норм и правил работы по обеспечению сохранности коммерческих секретов.
3. Организационные меры являются решающим звеном в формировании и реализации комплексных мер защиты информации. Они, в первую очередь, выражаются в создании службы безопасности коммерческого предприятия и обеспечении ее нормального функционирования.
4. Инженерно-техническая защита — это использование различных технических средств в интересах обеспечения информационной безопасности.

Глава 3 СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ [^]

*Если есть угроза — должны быть и средства
защиты и противодействия*

Способы — это порядок и приемы использования сил и средств для достижения поставленной цели по защите конфиденциальной информации.

Постулаты

1. Подальше положишь — поближе возьмешь.
2. Береженого Бог бережет.
3. На Бога надейся, а сам не плошай.
4. Сначала подумай, потом говори.
5. Не зная броду, не суйся в воду.
6. Семь раз отмерь, один раз отрежь.
7. Дело мастера боится.
8. Негоже, когда сапоги тачает пирожник, а пироги печет сапожник.
9. Отыщи всему начало, и ты многое поймешь (К. Прутков).

Любое действие человека, ориентированное на достижение каких-либо результатов, реализуется определенными способами. Естественно, что имеющийся опыт по защите информации достаточно четко определил совокупность приемов, сил и средств, ориентированных на обеспечение информационной безопасности. С учетом этого можно так определить понятие способов защиты информации: способы защиты информации — это совокупность приемов, сил и средств, обеспечивающих конфиденциальность, целостность, полноту и доступность информации и противодействие внутренним и внешним угрозам.

Естественно предположить, что каждому виду угроз присущи свои специфические способы, силы и средства.

3.1. Общие положения [^]

Обеспечение информационной безопасности достигается системой мер, направленных:

- на **предупреждение угроз**. Предупреждение угроз — это превентивные меры по обеспечению информационной безопасности в интересах упреждения возможности их возникновения;
- на **выявление угроз**. Выявление угроз выражается в систематическом анализе и контроле возможности появления реальных или потенциальных угроз и своевременных мерах по их предупреждению;
- на **обнаружение угроз**. Обнаружение имеет целью определение реальных угроз и конкретных преступных действий;
- на **локализацию** преступных действий и принятие мер по ликвидации угрозы или конкретных преступных действий;
- на **ликвидацию** последствий угроз и преступных действий и восстановление статус-кво (рис. 26).

Предупреждение возможных угроз и противоправных действий может быть обеспечено самыми различными мерами и средствами, начиная от создания климата глубоко осознанного отношения сотрудников к проблеме безопасности и защиты информации до создания глубокой, эшелонированной системы защиты физическими, аппаратными, программными и криптографическими средствами.

Предупреждение угроз возможно и путем получения (если хотите — и добывания) информации о готовящихся противоправных актах, планируемых хищениях, подготовительных действиях и других элементах преступных деяний. Для этих целей необходима работа сотрудников службы безопасности с инфор

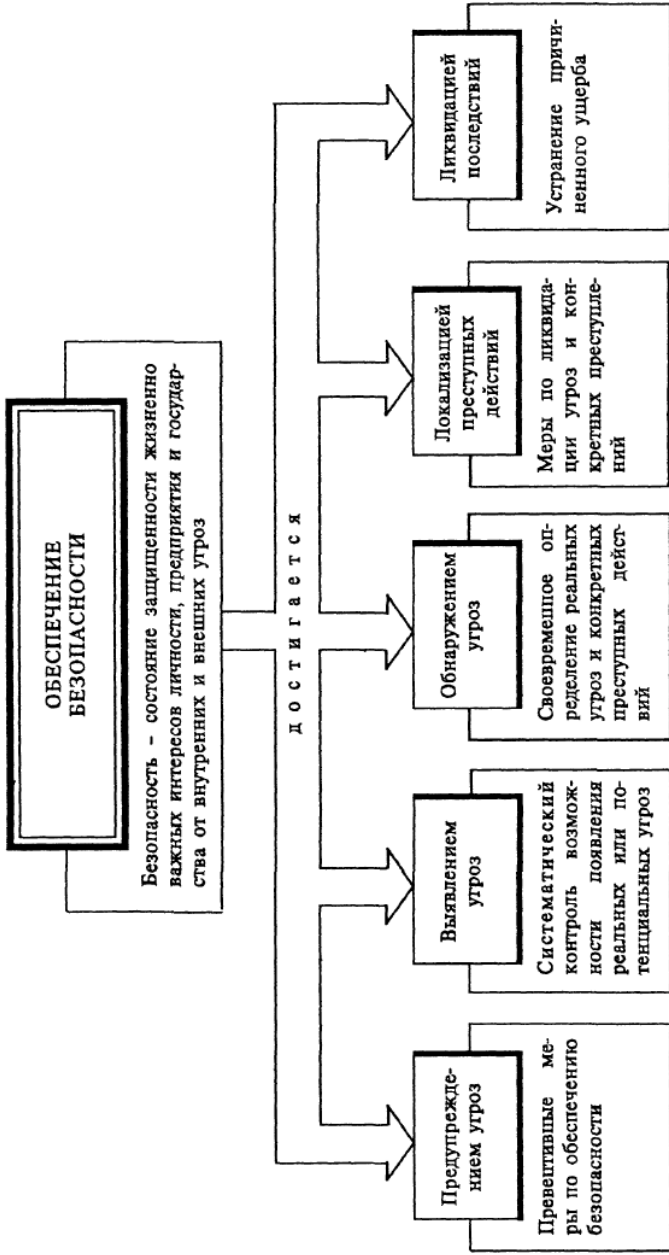


Рис. 26

маторами в интересах наблюдения и объективной оценки ситуации как внутри коллектива сотрудников, особенно главных участков ее фирмы, так и вне, среди конкурентов и преступных формирований.

В предупреждении угроз весьма существенную роль играет информационно-аналитическая деятельность службы безопасности на основе глубокого анализа криминогенной обстановки и деятельности конкурентов и злоумышленников.

Выявление имеет целью проведение мероприятий по сбору, накоплению и аналитической обработке сведений о возможной подготовке преступных действий со стороны криминальных структур или конкурентов на рынке производства и сбыта товаров и продукции. Особое внимание в этом виде деятельности должно отводиться изучению собственных сотрудников. Среди них могут быть и недовольные, и неопытные, и «внедренные».

Обнаружение угроз — это действия по определению конкретных угроз и их источников, приносящих тот или иной вид ущерба. К таким действиям можно отнести обнаружение фактов хищения или мошенничества, а также фактов разглашения конфиденциальной информации или случаев несанкционированного доступа к источникам коммерческих секретов. В числе мероприятий по обнаружению угроз значительную роль могут сыграть не только сотрудники службы безопасности, но и сотрудники линейных подразделений и служб фирмы, а также технические средства наблюдения и обнаружения правонарушений.

Пресечение или локализация угроз — это действия, направленные на устранение действующей угрозы и конкретных преступных действий. Например, пресечение подслушивания конфиденциальных переговоров за счет акустического канала утечки информации по вентиляционным системам.

Ликвидация последствий имеет целью восстановление состояния, предшествовавшего наступлению угрозы. Например, возврат долгов со стороны заемщиков. Это может быть и задержание преступника с украденным имуществом, и восстановление разрушенного здания от подрыва, и другое.

Все эти способы имеют целью защитить информационные ресурсы от противоправных посягательств и обеспечить:

- предотвращение разглашения и утечки конфиденциальной информации;
- воспреещение несанкционированного доступа к источникам конфиденциальной информации;

- сохранение целостности, полноты и доступности информации;
- соблюдение конфиденциальности информации;
- обеспечение авторских прав (рис. 27).

Защита от разглашения сводится в общем плане к разработке перечня сведений, составляющих коммерческую тайну предприятия. Эти сведения должны быть доведены до каждого сотрудника, допущенного к ним, с обязательством этого сотрудника сохранять коммерческую тайну. Одним из важных мероприятий является система контроля за сохранностью коммерческих секретов.

Защита от утечки конфиденциальной информации сводится к выявлению, учету и контролю возможных каналов утечки в конкретных условиях и к проведению организационных, организационно-технических и технических мероприятий по их ликвидации.

Защита от несанкционированного доступа к конфиденциальной информации обеспечивается путем выявления, анализа и контроля возможных способов несанкционированного доступа и проникновения к источникам конфиденциальной информации, и реализацией организационных, организационно-технических и технических мероприятий по противодействию НСД(рис. 28).

На практике в определенной степени все мероприятия по использованию технических средств защиты информации подразделяются на три группы:

- организационные (в части технических средств);
- организационно-технические;
- технические.

Организационные мероприятия — это мероприятия ограничительного характера, сводящиеся в основном к регламентации доступа и использования технических средств обработки информации. Они, как правило, проводятся силами самой организации путем использования простейших организационных мер.

В общем плане организационные мероприятия предусматривают проведение следующих действий:

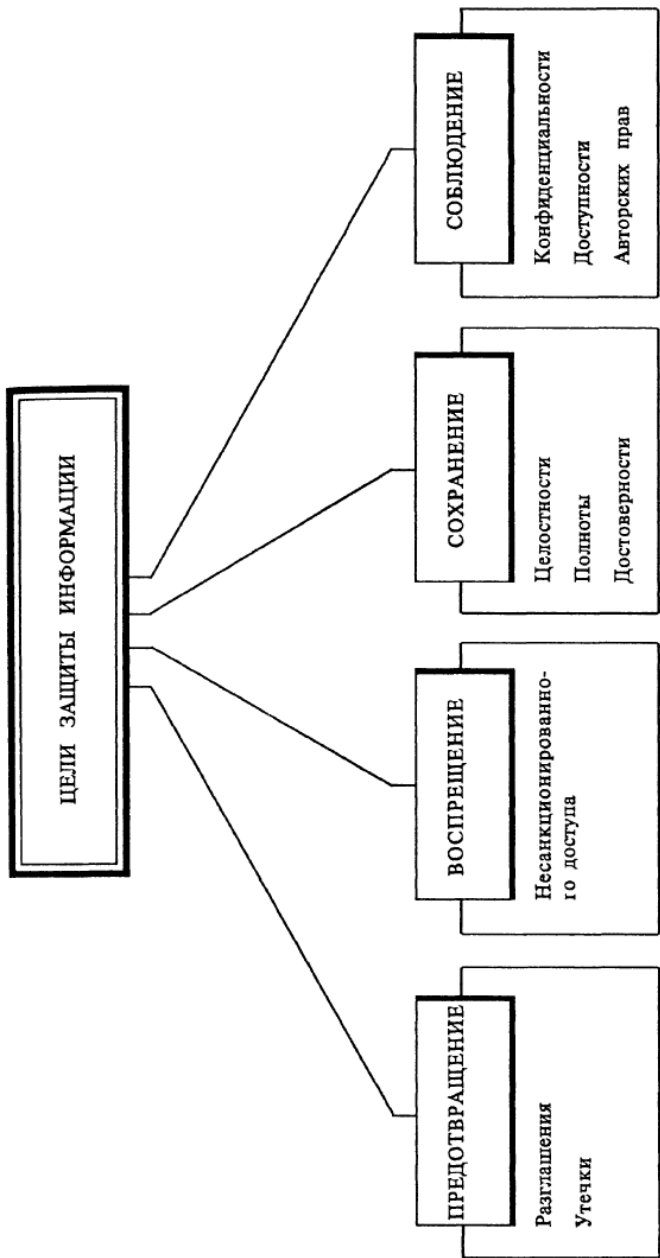


Рис 27

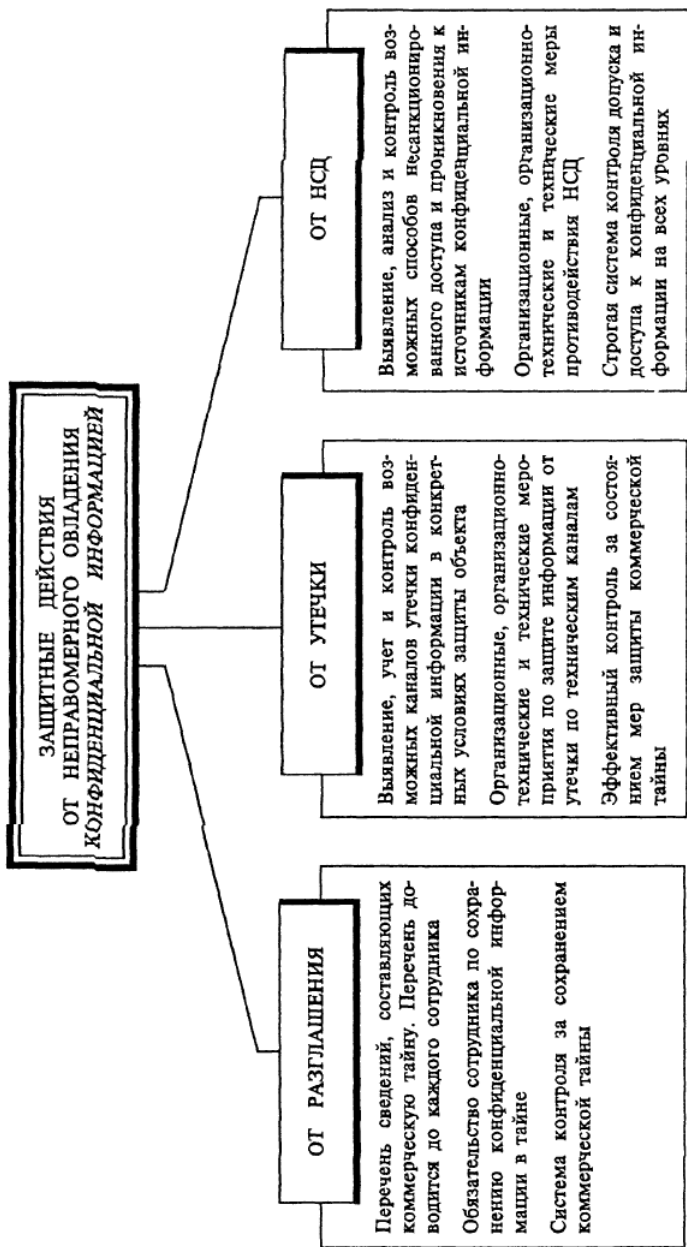


Рис. 28

- определение границ охраняемой зоны (территории);
- определение технических средств, используемых для обработки конфиденциальной информации в пределах контролируемой территории;
- определение «опасных», с точки зрения возможности образования каналов утечки информации, технических средств и конструктивных особенностей зданий и сооружений;
- выявление возможных путей проникновения к источникам конфиденциальной информации со стороны злоумышленников;
- реализация мер по обнаружению, выявлению и контролю за обеспечением защиты информации всеми доступными средствами (рис. 29).

Организационные мероприятия выражаются в тех или иных ограничительных мерах. Можно выделить такие ограничительные меры, как территориальные, пространственные и временные.

Территориальные ограничения сводятся к умелому расположению источников на местности или в зданиях и помещениях, исключающих подслушивание переговоров или перехват сигналов радиоэлектронных средств.

Пространственные ограничения выражаются в выборе направлений излучения тех или иных сигналов в сторону наименьшей возможности их перехвата злоумышленниками.

Временные ограничения проявляются в сокращении до минимума времени работы технических средств, использовании скрытых методов связи, шифровании и других мерах защиты (рис. 30).

Одной из важнейших задач организационной деятельности является определение состояния технической безопасности объекта, его помещений, подготовка и выполнение организационных мер, исключающих возможность неправомерного овладения конфиденциальной информацией, воспреещение ее разглашения, утечки и несанкционированного доступа к охраняемым секретам.

Организационно-технические мероприятия обеспечивают блокирование разглашения и утечки конфи

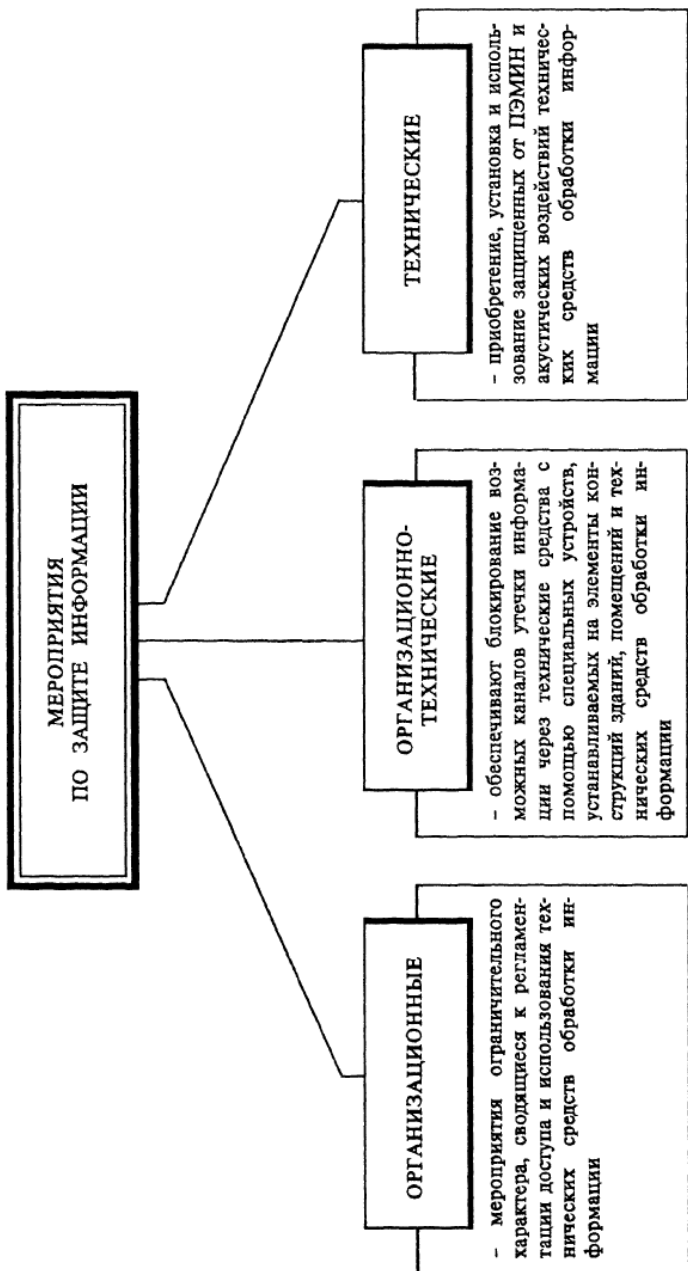


Рис. 29

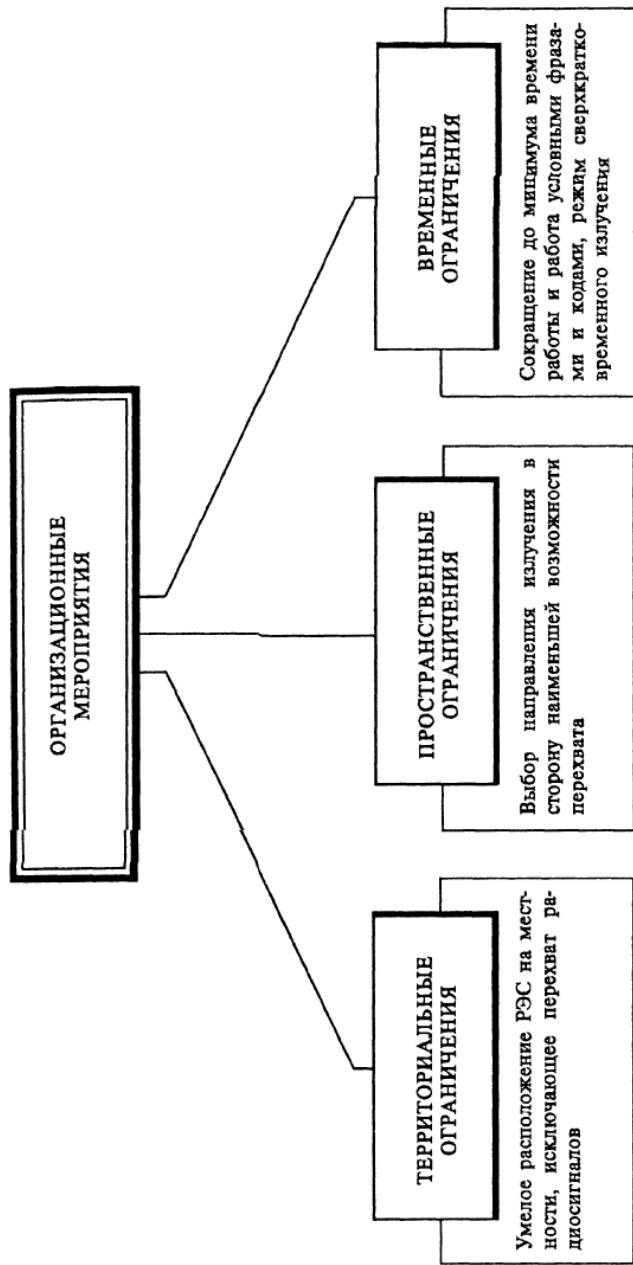


Рис. 30

денциальных сведений через технические средства обеспечения производственной и трудовой деятельности, а также противодействие техническим средствам промышленного шпионажа с помощью специальных технических средств, - устанавливаемых на элементы конструкций зданий, помещений и технических средств, потенциально образующих каналы утечки информации. В этих целях возможно использование:

- технических средств пассивной защиты, например, фильтров, ограничителей и тому подобных средств развязки акустических, электрических и электромагнитных систем защиты сетей телефонной связи, энергоснабжения, радио- и часофикации;
- технических средств активной защиты: датчиков акустических шумов и электромагнитных помех.

Организационно-технические мероприятия по защите информации можно подразделить на пространственные, режимные и энергетические.

Пространственные меры выражаются в уменьшении ширины диаграммы направленности, ослаблении боковых и заднего лепестков диаграммы направленности излучения радиоэлектронных средств (РЭС).

Режимные меры сводятся к использованию скрытых методов передачи информации по средствам связи: шифрование, квазипеременные частоты передачи и других.

Энергетические — это снижение интенсивности излучения и работа РЭС на пониженных мощностях (рис. 31).

Технические мероприятия — это мероприятия, обеспечивающие приобретение, установку и использование в процессе производственной деятельности специальных, защищенных от побочных излучений (безопасных) технических средств или средств, ПЭМИН которых не превышают границу охраняемой территории.

Технические мероприятия по защите конфиденциальной информации можно подразделить на скрытие, подавление и дезинформацию.

Скрытие выражается в использовании радиомолчания и создании пассивных помех приемным средствам злоумышленников.

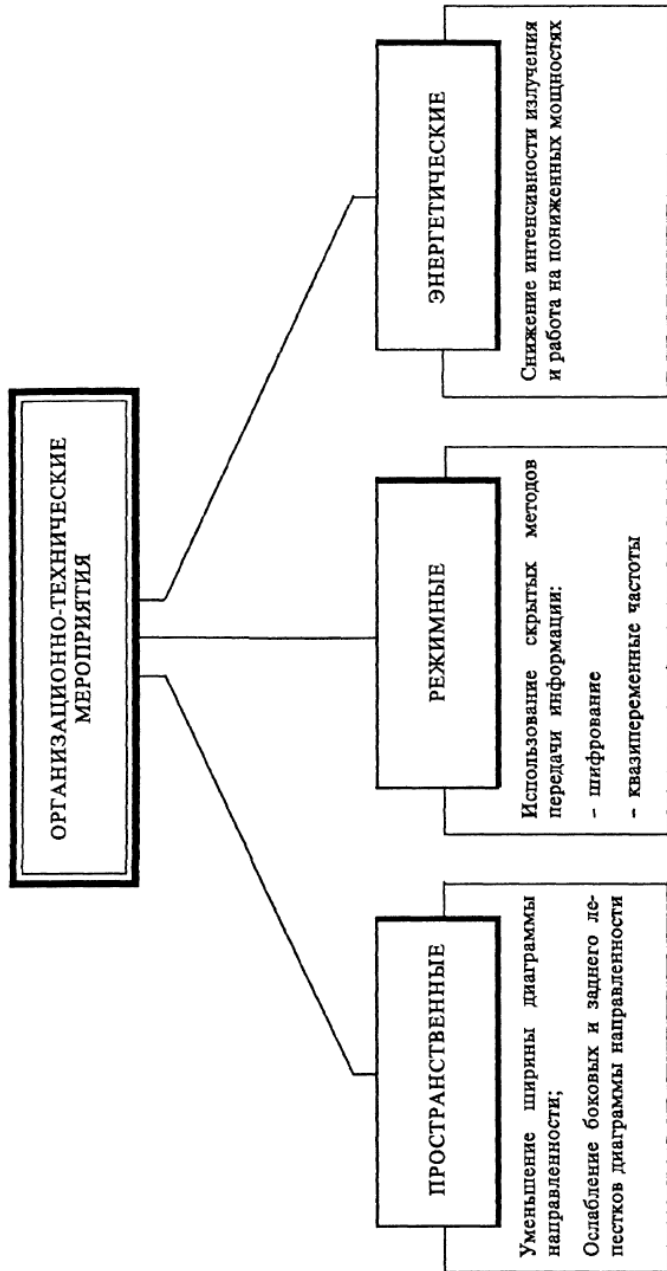


Рис. 31

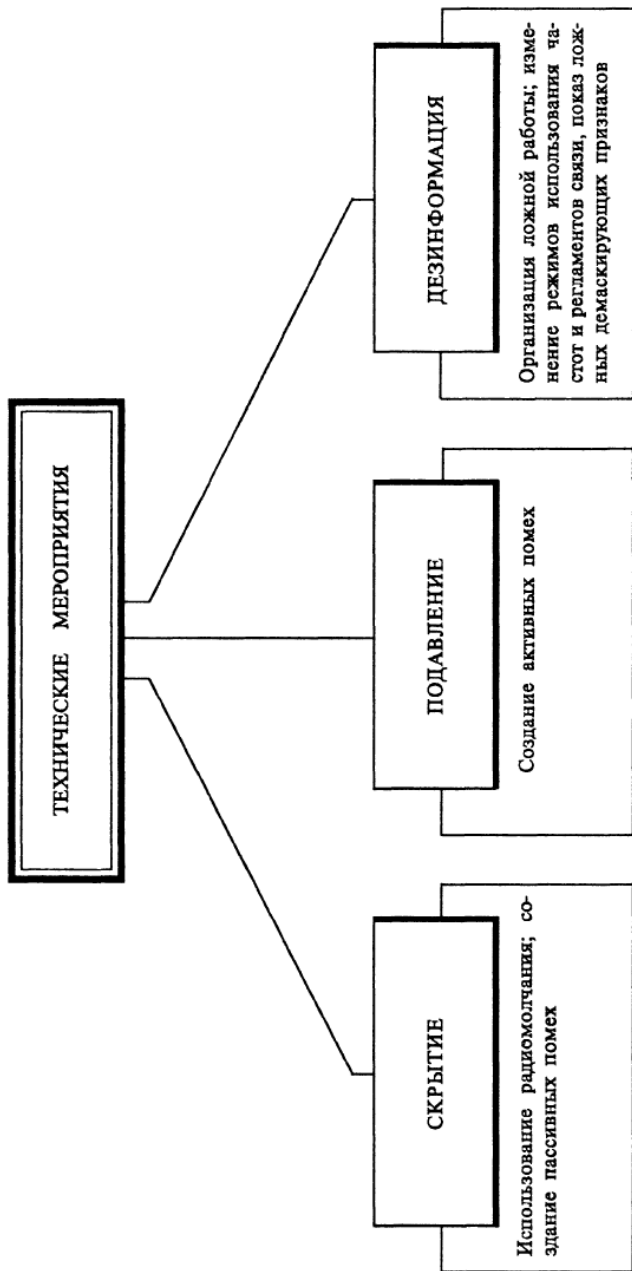


Рис 32

Подавление — это создание активных помех средствам злоумышленников.

Дезинформация — это организация ложной работы технических средств связи и обработки информации; изменение режимов использования частот и регламентов связи; показ ложных демаскирующих признаков деятельности и опознавания.

Защитные меры технического характера могут быть направлены на конкретное техническое устройство или конкретную аппаратуру и выражаться в таких мерах, как отключение аппаратуры на время ведения конфиденциальных переговоров или использование тех или иных защитных устройств типа ограничителей, буферных средств, фильтров и устройств зашумления (рис. 32).

3.2. Характеристика защитных действий [^]

Защитные действия ориентированы на пресечение разглашения, защиту информации от утечки и противодействия несанкционированному доступу (рис. 33).

Защитные действия по обеспечению информационной безопасности можно классифицировать по основным характеристикам и объектам защиты по таким параметрам, например, как ориентация, характер угроз, направления, способы действий, охват, масштаб и другим.

Защитные действия по ориентации можно классифицировать как действия, направленные на защиту персонала, материальных и финансовых средств и информации как ресурса.

По направлениям — это правовая, организационная и инженерно-техническая защита.

По способам — это предупреждение, выявление, обнаружение, пресечение и восстановление.

По охвату защитные меры могут быть ориентированы на защиту территории фирмы, зданий, отдельных (выделенных) помещений, конкретных видов аппаратуры, или технических средств и систем, или отдельных элементов зданий, помещений, аппаратуры, опасных с точки зрения несанкционированного доступа к ним, или оборудования каналов утечки информации.

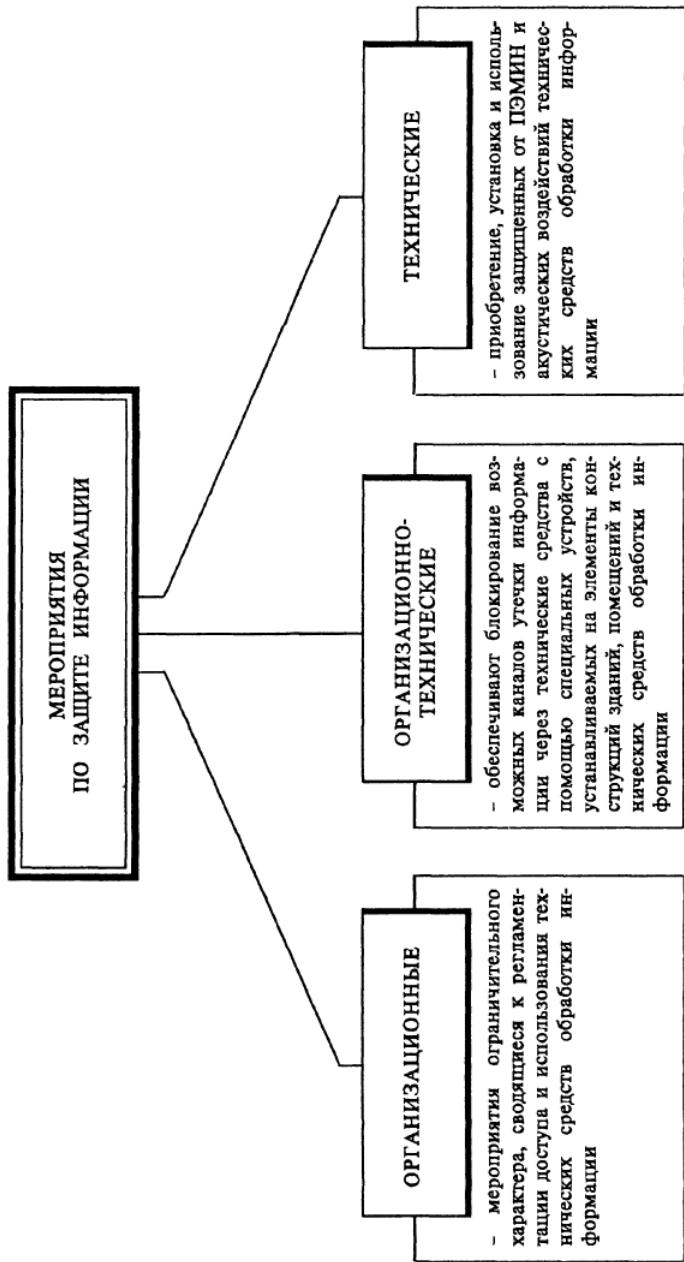


Рис. 33

Применение защитных мер можно рассматривать и в пространственном плане. Так, например, известно, что распространение (разглашение, утечка или НСД) осуществляется от источника информации через среду к злоумышленнику (рис. 34).

Источником информации могут быть люди, документы, технические средства, отходы и другое. Носителем информации может быть либо поле (электромагнитное, акустическое), либо вещество (бумага, материал, изделие и т. д.). Средой является воздушное пространство, жесткие среды (стены, коммуникации).

Злоумышленник обладает необходимыми средствами приема акустической и электромагнитной энергии, средствами воздушного наблюдения и возможностью обрабатывать материально-вещественные формы представления информации.

Чтобы исключить неправомерное овладение конфиденциальной информацией, следует локализовать (выключить, ослабить сигнал, зашифровать) источник информации.

С увеличением масштабов распространения и использования ПЭВМ и информационных сетей усиливается роль различных факторов, вызывающих утечку, разглашение и несанкционированный доступ к информации. К ним относятся:

- несанкционированные и злоумышленные действия персонала и пользователя;
- ошибки пользователей и персонала;
- отказы аппаратуры и сбои в программах;
- стихийные бедствия, аварии различного рода и опасности.

В соответствии с этим основными целями защиты информации в ПЭВМ и информационных сетях являются:

- обеспечение юридических норм и прав пользователей в отношении ДОСТУПА к информационным и другим сетевым ресурсам, предусматривающее административный надзор за информационной деятельностью, включая меры четкой персональной ответственности за соблюдение правил пользования и режимов работы;
- предотвращение потерь и утечки информации, перехвата и вмешательства на всех уровнях, для всех территориально разделенных объектов;

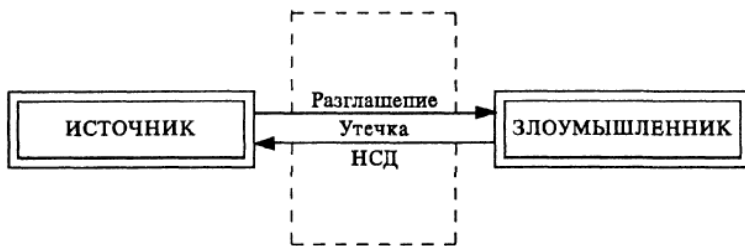


Рис 34

- обеспечение целостности данных на всех этапах и фазах их преобразования и сохранности средств программного обеспечения.

В связи с тем, что информационная сеть, в отличие от автономной ПЭВМ, является территориально распределенной системой, она требует принятия специальных мер и средств защиты. Средства защиты должны предотвращать:

- определение содержания передаваемых сообщений;
- внесение изменений в сообщения;
- необоснованный отказ в доступе;
- несанкционированный доступ;
- ложную инициализацию обмена;
- возможность измерения и анализа энергетических и других характеристик информационной системы.

Если это нецелесообразно или невозможно, то нарушить информационный контакт можно за счет использования среды распространения информации. Например, при почтовой связи использовать надежного связного и доставить почтовое отправление абоненту, полностью исключив возможность несанкционированного доступа к нему со стороны. Или исключить возможность подслушивания путем использования специального помещения, надежно защищенного от такого вида НСД. И, наконец, можно воздействовать на злоумышленника или на его средства путем постановки активных средств воздействия (помехи).

В каждом конкретном случае реализации информационного контакта используются и свои специфические способы воздействия как на источник, так и на среду и на злоумышленника. В качестве примера рассмотрим матрицу, характеризующую взаимосвязь целей защиты информации и механизмов ее защиты в процессе телекоммуникационного обмена в распределенных автоматизированных системах (табл. 3). Одно-

Таблица 3

временно на ней отражены и защитные возможности тех или иных механизмов.

| ЦЕЛИ ЗАЩИТЫ | СОДЕРЖАНИЕ | МЕХАНИЗМЫ ЗАЩИТЫ | | | | | | | | |
|-------------------------------|--|------------------|------------------|---------------------|--------------------------------|-----------------------|---|---------------------------|---------------|---|
| | | Шифрование | Цифровая подпись | Управление доступом | Обеспечение целостности данных | Аутентификация обмена | Полержание потока сообщений фиктивной информацией | Управление маршрутизацией | Подтверждение | |
| Соблюдение конфиденциальности | Область безопасности | ● | - | - | - | - | - | - | - | - |
| | Предварительное засекречивание | ● | - | - | - | - | - | - | ● | - |
| | Линейное засекречивание | ● | - | - | - | - | - | - | ● | - |
| | Безопасность обмена | ● | - | - | - | - | - | - | ● | - |
| Обеспечение целостности | Безотносительные области безопасности | ● | ● | - | ● | - | - | - | - | - |
| | Безотносительная целостность | ● | ● | - | ● | - | - | - | - | - |
| | Относительная область безопасности | ● | - | - | ● | - | - | - | - | - |
| | Связанная целостность с восстановлением | ● | - | - | ● | - | - | - | - | - |
| Подтверждение целостности | Связанная целостность без восстановления | ● | - | - | ● | - | - | - | - | - |
| | Каждого сообщения | ● | ● | - | - | ● | - | - | - | - |
| | Источника информации | ● | ● | - | - | - | - | - | - | - |
| | Управления доступом | - | - | ● | - | - | - | - | - | - |
| Подтверждение | Факта отправления | - | ● | - | ● | - | - | - | - | ● |
| | Местонахождения отправителя | - | ● | - | ● | - | - | - | - | ● |

Выводы

1. Многообразие условий, способствующих неправомерному овладению конфиденциальной информацией, вызывает необходимость использования не менее многообразных способов, сил и средств для обеспечения информационной безопасности.
2. Способы обеспечения информационной безопасности должны быть ориентированы на упреждающий характер действий, направляемых на заблаговременные меры предупреждения возможных угроз коммерческим секретам.
3. Основными целями защиты информации являются обеспечение конфиденциальности, целостности, полноты и достаточности информационных ресурсов.
4. Обеспечение информационной безопасности достигается организационными, организационно-техническими и техническими мероприятиями, каждое из которых обеспечивается специфическими силами, средствами и мерами, обладающими соответствующими характеристиками.
5. Совокупность способов обеспечения информационной безопасности может быть подразделена на общие и частные, применение которых обуславливается масштабностью защитных действий.

Глава 4 ПРЕСЕЧЕНИЕ РАЗГЛАШЕНИЯ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ [^]

Люби молчать, нежели говорить

Пресечение разглашения конфиденциальной информации — это комплекс мероприятий, исключающих оглашение охраняемых сведений их владельцами.

Постулаты

1. Мудр тот, кто умеет молчать.
2. Слово — серебро, молчание — золото.
3. Что у трезвого на уме, то у пьяного на языке.
4. Язык мой — враг мой.
5. Ешь суп с грибами и держи язык за зубами.
6. Слово — не воробей, вылетит — не поймаешь.
7. Нет ничего смутительнее многословия и зловреднее невоздержанного языка.
8. Наблюдающий за языком своим вовек не будет им обкраден.

Помня, что «болтун — находка для шпиона», следует учесть, что из всех условий, способствующих неправомерному овладению конфиденциальной информацией, излишняя болтливость собственных сотрудников фирмы составляет 32%. Это третья часть. Если еще добавить, что безответственный обмен опытом составляет 12%, то получается, что разглашение коммерческих секретов составляет почти половину (42%) угроз конфиденциальной информации. Это уже очень плохо!

Умышленное разглашение производственных секретов обходится экономике США в 2 миллиарда долларов ежемесячно. Как установило в ходе недавнего опроса предприятий американское общество промышленной безопасности (АСИС), число подобных инцидентов с 1993 года утроилось.

Причин этого роста несколько. Лояльность одних служащих

подрывает ужесточение дисциплины, других — перекупают конкуренты. Это касается в первую очередь высокотехнологичных отраслей.

К конкурентам частенько попадают материалы о стратегии предприятий, результаты исследовательских и опытно-конструкторских работ, списки клиентов, заявки на патенты, торговые марки и авторские права.

4.1. Общие положения [^]

Напомним, что РАЗГЛАШЕНИЕ — это умышленные или неосторожные действия должностных лиц и граждан, результатом которых явилось неправомерное оглашение конфиденциальных сведений, и как следствие — ознакомление с ними лиц, не допущенных к этим сведениям. Выражается разглашение в сообщении, передаче, предоставлении, пересылке, опубликовании, утере и иных способах обмена деловой и научной информацией.

С точки зрения инициативы образование информационного контакта и степени участия в нем компонентов коммуникации активной стороной выступает источник, т. е. владелец информации.

Считается, что разглашение охраняемой информации может произойти при наличии ряда условий и обстоятельств служебного и личного характера. Причины разглашения, как правило, связаны с несовершенством разработанных норм по защите информации, а также нарушением этих норм (в том числе и несовершенных), отступлением от правил обращения с соответствующими документами и сведениями, содержащими конфиденциальную информацию.

К факторам и обстоятельствам, приводящим к разглашению информации, относятся:

- недостаточное знание сотрудниками правил защиты конфиденциальной информации и непонимание (или недопонимание) необходимости тщательного их выполнения;
- слабый контроль за соблюдением правил работы со сведениями конфиденциального характера;
- текучесть кадров, в том числе знающих сведения конфиденциального характера (рис. 35).

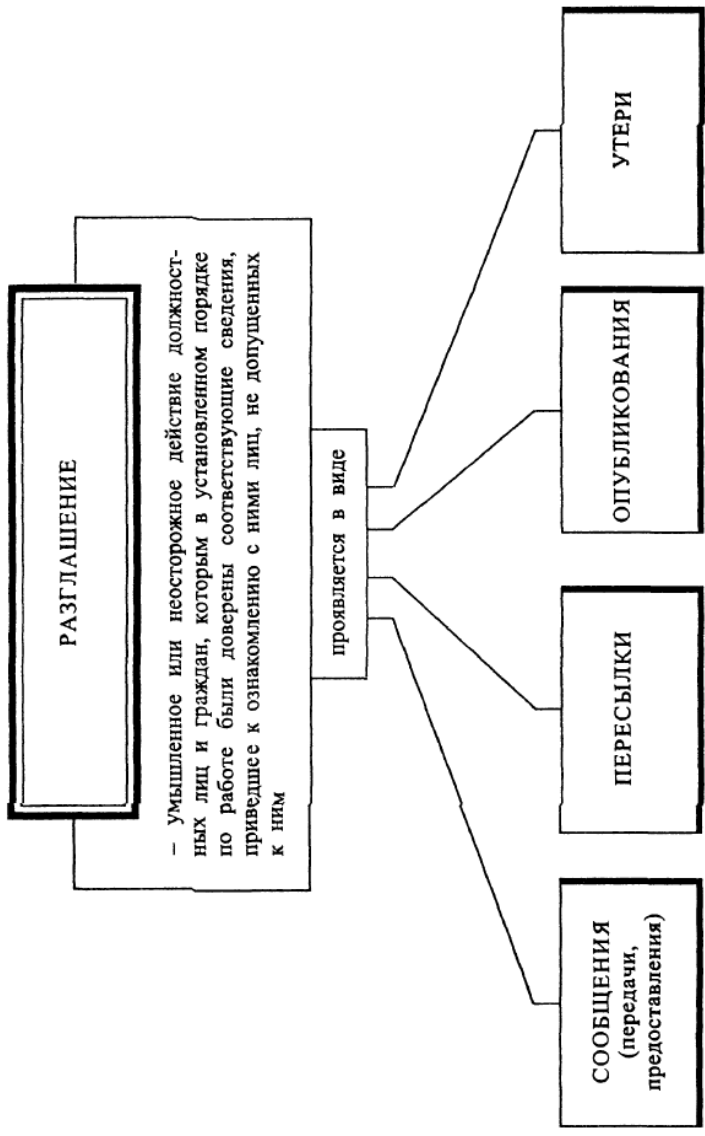


Рис. 35

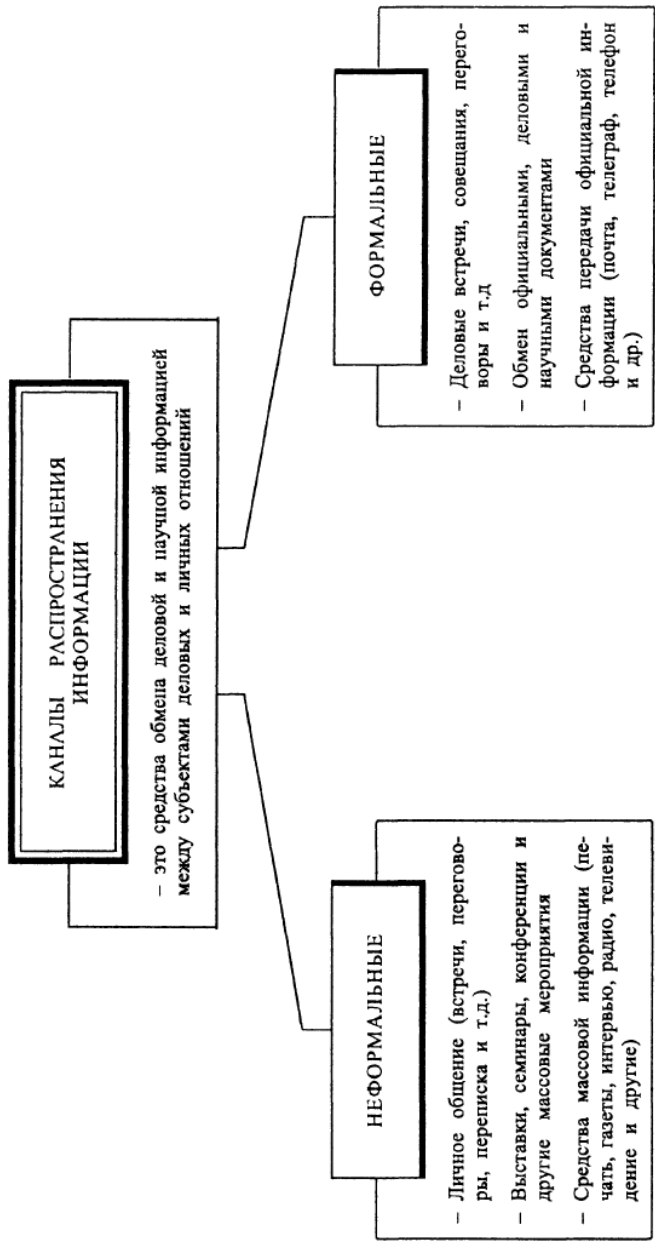


Рис. 36

Разглашение конфиденциальной информации возможно

1. При передаче информации по каналам электросвязи
 2. При сообщении, оглашении
 - на деловых встречах и переговорах,
 - при деловой переписке,
 - на семинарах, симпозиумах, в печати и СМИ,
 - на выставках,
 - в судебных инстанциях и административных органах
 3. При пересылке документов
 - по каналам почтовой связи,
 - нарочными, курьерами, попутчиками
 4. При опубликовании
 - в печати,
 - в научных исследованиях и диссертациях
 5. При личном общении
 - на встречах,
 - при телефонных переговорах
 6. При утере, утрате документов
 - на работе,
 - за пределами службы
 7. При бесконтрольном оставлении документов.
 - на рабочем месте,
 - на экране ПЭВМ,
 - при ксерокопировании
 8. При бесконтрольной разработке документов
 - необоснованное изготовление документов,
 - включение в обычные документы сведений конфиденциального характера,
 - черновики, наброски, испорченные варианты
 9. При бесконтрольном документообороте
 - необоснованная рассылка документов,
 - необоснованное ознакомление с документами сотрудников и соисполнителей
 10. При бесконтрольном хранении и уничтожении документов
 11. При бесконтрольном приеме поступающей документации
- Известны формальные и неформальные каналы распространения информации (рис 36)

Это лишь беглое ознакомление с возможными направлениями, условиями и действиями, приводящими к разглашению конфиденциальной информации.

В жизни таких условий и направлений значительно больше и рассматривать их необходимо на конкретных объектах.

В основу защиты информации от разглашения, целесообразно положить:

1. Принцип максимального ограничения числа лиц, допущенных к работе с конфиденциальной информацией, так как степень ее сохранности находится в прямой зависимости от числа допущенных к ней лиц.
2. Принцип персональной ответственности за сохранность информации предполагает разработку мер, побуждающих сотрудников хранить секреты не только из-за боязни последствий за вольное или невольное раскрытие, но и обеспечивающих за заинтересованность каждого конкретного работника в сохранении тайны.

Отсюда одним из направлений работы является работа с кадрами, воспитательно-профилактическая деятельность, которая включает в себя совокупность методов воздействия на сознание, чувство, волю и характер сотрудников в интересах формирования у них умения хранить тайну и строго соблюдать установленные правила работы с закрытой информацией. Главные направления этой деятельности:

- привитие навыков предупреждения разглашения конфиденциальной информации;
- повышение ответственности за сохранение секретов;
- создание обстановки нетерпимости к фактам нарушения установленного порядка обеспечения информационной безопасности;
- строгий контроль за всеми видами переговоров со сторонними организациями и их представителями;
- контроль публикаций, выступлений, интервью и других форм общения по вопросам деятельности предприятия;
- контроль разговоров в служебных помещениях и телефонных переговоров сотрудников на служебные темы;
- изучение действий и поведения сотрудников во внеслужебное время, мест их пребывания, наклонностей, увлечений, пагубных привычек, трудового удовлетворения и другие.

Естественно, что все эти действия должны проводиться в строгом соответствии с законодательными актами, с точным

соблюдением прав и обязанностей сотрудников предприятия, без какого-либо вмешательства в личную жизнь.

Подобные действия могут выполнять, например, частные детективы (сотрудники службы безопасности). Согласно Закону РФ «О частной детективной и охранной деятельности», им разрешается осуществлять следующие виды услуг:

1. Сбор сведений по гражданским делам.
2. Изучение рынка.
3. Сбор сведений о партнерах и конкурентах.
4. Выявление недобросовестных и неплатежеспособных партнеров.
5. Установление обстоятельств недобросовестной конкуренции.
6. Установление обстоятельств разглашения коммерческих секретов.

Эти услуги реализуются с целью:

1. Поиска без вести пропавших.
2. Поиска утраченного имущества.
3. Выявления биографических данных, характеризующих граждан.
4. Изучения сведений по уголовным делам и другое.

При этом частному детективу разрешается:

1. Устный опрос граждан и должностных лиц с их согласия.
2. Изучение предметов и документов с согласия их владельцев.
3. Наведение справок.
4. Внешний осмотр помещений и других объектов.
5. Наблюдение для получения необходимой информации.
6. Использование видео- и аудиозаписи, кино- и фотосъемки, технических и иных средств, не причиняющих вреда гражданам, оперативной связи.
7. Использование специальных средств личной безопасности.

Опыт работы по пресечению разглашения конфиденциальной информации позволяет разработать определенную систему мер по предотвращению разглашения на общем уровне рекомендаций в виде типового классификатора защитных действий по предотвращению разглашения конфиденциальной информации. Такой документ может быть детальным, если он будет привязан к конкретному объекту с акцентом на местные условия, учетом

имеющихся средств, особенностей зданий и помещений.

В качестве примера приведен вариант «Каталога защитных действий по пресечению разглашения конфиденциальной информации» на общем уровне рекомендаций (см. Приложение 14).

С целью придания «Каталогу» практической значимости в интересах повседневного использования служба безопасности должна внести в него конкретные мероприятия с привязкой к конкретным условиям.

Деятельность руководства предприятия и сотрудников службы безопасности по предупреждению разглашения охраняемых сведений включает в себя и обучение сотрудников, ознакомление их с законами, постановлениями, положениями, инструкциями, определяющими правовое отношение с государством и предприятием.

Значительное место в работе с персоналом должно отводиться обучению методам и мерам обеспечения сохранности ценной информации. В процессе обучения необходимо добиваться, чтобы сотрудники четко знали категории охраняемых ими сведений, ценность этих данных, возможные способы и методы проникновения со стороны нарушителей, а также правила и процедуры их защиты. Следует особо обратить внимание на то, чтобы сотрудники осознанно понимали разумность и необходимость всех действующих элементов режима сохранения секретов.

Следует использовать любую возможность для пропаганды обеспечения экономической безопасности предприятия; не забывать периодически вознаграждать сотрудников фирмы за успехи в этой работе; всемерно стимулировать заинтересованность и участие сотрудников в выполнении программы по обеспечению безопасности.

4.2. Способы пресечения разглашения [^]

Важной составляющей обеспечения информационной безопасности фирмы является контроль лояльности ее персонала. Такая работа проводится как в целях упреждения преступных посягательств, так и для расследования конкретных случаев нанесения ущерба.

Неотъемлемая часть этой работы — мониторинг телефонных переговоров, ведущихся из офиса. Осуществляется также акустический или визуально-акустический контроль разговоров и

действий в служебных помещениях.

Микрофонные системы акустического контроля бывают одноканальные и многоканальные. Используются мало- или микрогабаритные микрофоны, монтируемые скрытно, соединенные проводами с приемными средствами и средствами магнитной записи. Часто вблизи самого микрофона устанавливается малогабаритный усилитель с автономным или дистанционным питанием.

Многоканальные системы акустического контроля объединяют несколько (от 2 до 16 и более) одноканальных устройств в комплексе. Центральной частью такого комплекса является концентратор, обеспечивающий коммутацию необходимых каналов, выбор режима контроля, запись сигналов на магнитофоны и прослушивание переговоров на встроенные динамики или головные телефоны. В качестве примера рассмотрим состав концентратора акустического контроля на четыре канала. Он имеет следующие возможности:

- количество каналов — 4;
- диапазон воспроизводимых частот — 30 Гц — 10 кГц;
- выходная мощность — 0,2 Вт.

Сканер представляет собой, кроме коммутатора, еще и усилитель низкой частоты с широкими возможностями регулировки уровня сигнала, регулировки НЧ и ВЧ полосы, системой автоматического сканирования каналов. В состав сканера входят магнитофоны для обеспечения записи акустических сигналов в режиме контроля.

Расстояние от микрофонов до концентратора определяется конкретным изделием и может варьироваться от 300 до 3 — 5 тыс. метров. Концентратор устанавливается на посту контроля службы безопасности фирмы и позволяет прослушивать и записывать на аудиомикрофон любой из контролируемых микрофонов.

Аудиозапись ведется на специальные магнитофоны. Например, компактный магнитофон типа CRAJG J-109 предназначен для записи аудиосигналов в течение 10 часов (непрерывная запись в течение 3 часов) на стандартную кассету С-120. Магнитофон имеет систему активизации записи голосом (VOX) с регулировкой низкого и высокого порогов срабатывания, что значительно увеличивает общее время записи. Имеется встроенный микрофон, счетчик ленты.

При мониторинге телефонных переговоров требуется иная аппаратура. При этом возможно использование как мобильных, так

и стационарных средств. Последние можно подразделить на две основные группы:

- телефонные коммутаторы;
- автоматические системы мониторинга.

Понимая всю важность соблюдения конфиденциальности мониторинга телефонных переговоров в пределах конкретного предприятия, Правительством РФ 22 марта 1995 г. было принято Постановление № 291, в котором указывается: «Лица, участвующие в мониторинге, обязаны сохранять государственную и коммерческую тайну, к которой они получили доступ».

Телефонные коммутаторы используются для контроля небольшого числа телефонных линий (как правило, не более 20). Это стандартные изделия, выпускаемые в значительных количествах, имеющие определенный набор, позволяющий решить задачу мониторинга телефонных переговоров небольшого офиса. В качестве примера можно привести стационарный комплекс контроля телефонных переговоров «КТС-8» (фирмы «Гротек») (рис. 37).

«КТС-8» позволяет прослушивать телефонные переговоры на любой из 8 линий и производить автоматическую запись двух из них на диктофоны.

Однако такие устройства не обеспечивают эффективный контроль при значительном количестве телекоммуникационных точек в офисе, и тем более — в случае нали-

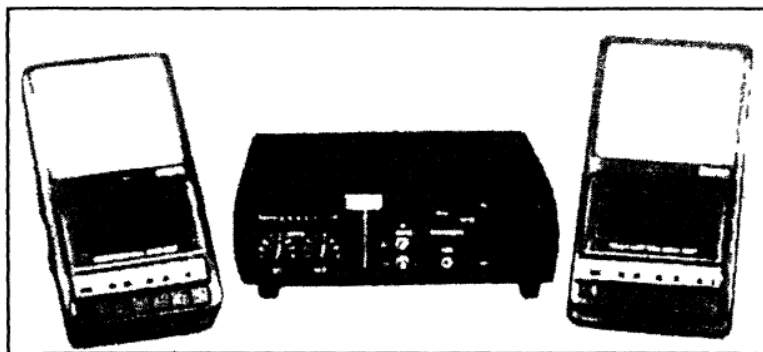


Рис 37

чия в организации офисной телефонной станции. Эта задача решается с помощью автоматических систем мониторинга. В литературе (Кашеев В.И. Мониторинг телефонной сети) показан пример такой системы. Состав ее приведен на рис. 38.

Рассмотренные средства предполагают контроль со стороны службы безопасности за сотрудниками и их абонентами в целях выявления возможного разглашения ими коммерческих секретов. Однако неэтично контролировать свое собственное руководство (например, генерального директора). В этом случае следует обеспечить индивидуальную запись телефонных разговоров первого лица в интересах самоконтроля (текущего и ретроспективного) на случайное (непреднамеренное) разглашение информации самим руководителем или его абонентами. Для этого используется перспективный диктофон типа MARANTZ PMD-201. Это профессиональный кассетный магнитофон, предназначенный для записи телефонных разговоров с микрофона или линейного входа. Используется стандартная кассета С-120. Запись длительностью до 4 часов. Питание от сети и от батареек, плавная регулировка скорости воспроизведения, регулятор тембра, встроенный микрофон, гнездо для подключения телефонной линии, счетчик ленты. Имеет гнездо для дистанционного включения

Для целей самоконтроля возможно использование любых других магнитофонов и диктофонов, имеющих гнездо подключения телефонной линии.

Магнитофонная запись сегодня признается как подтверждающий материал не только в деятельности

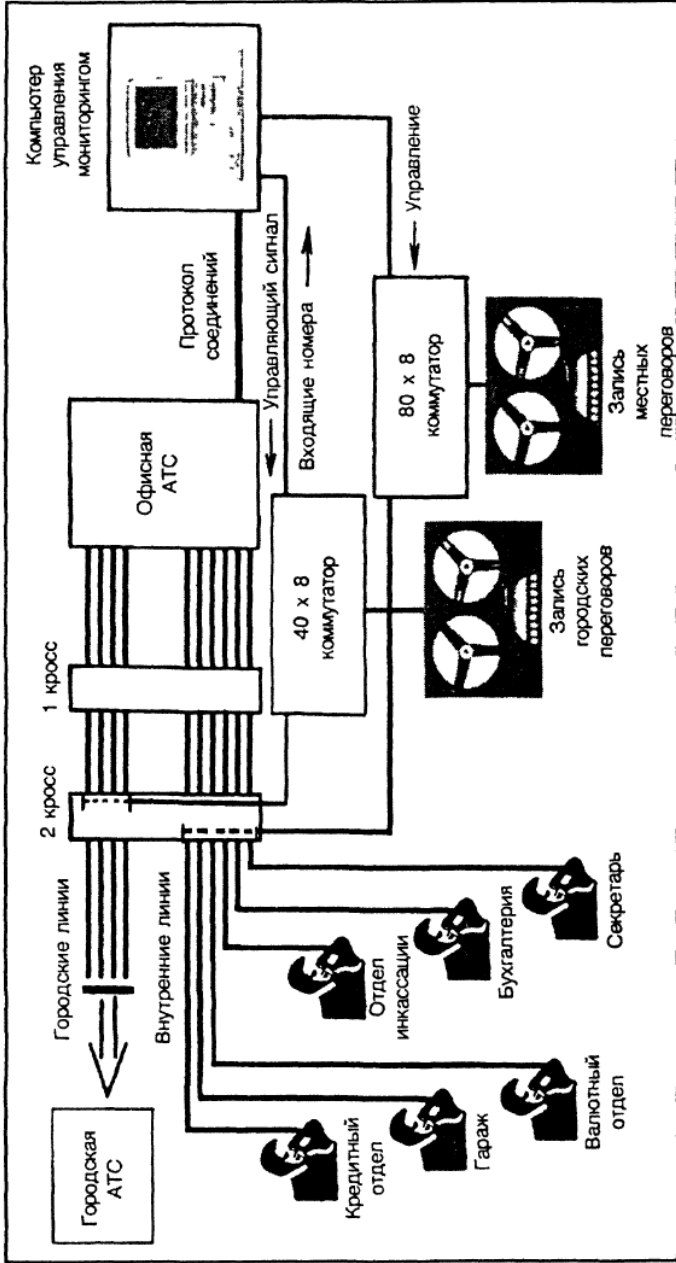


Рис. 38. Автоматическая система мониторинга телефонных переговоров

службы безопасности, но и в судебной практике. В этом случае целесообразно вести такую запись при ведении «сомнительных» телефонных переговоров (выпытывание, угрозы), такие записи могут помочь при расследовании и даже при судебных разбирательствах. Так, в газете «Московская правда» 28 сентября 1993 г. в статье ««Помог» уладить конфликт» сказано: «...вина подсудимого была подтверждена материалами дела и в их числе звукозаписями телефонных разговоров между потерпевшей и подсудимым. В этих разговорах Н подтверждал требование денег, говорил о возможности уничтожения имущества и о том, что имеет оружие».

Сейчас магнитные фонограммы прочно вошли в уголовный процесс как вещественное доказательство. Суды всех без исключения инстанций (в том числе и с участием присяжных заседателей) принимают магнитные фонограммы как неоспоримое доказательство по делу.

Экспертизу подлинности зафиксированной на пленке информации проводят эксперты экспертно-криминалистического центра МВД России. Почти во всех МВД, УВД созданы лаборатории видеофоноско-пических экспертиз и исследований.

Выводы

1. Разглашение конфиденциальной информации является наиболее распространенным действием, приводящим к неправомерному оглашению охраняемых сведений.
2. К факторам и обстоятельствам, приводящим к разглашению информации, относятся:
 - a. недостаточная подготовленность сотрудников к соблюдению требований по защите конфиденциальной информации;
 - b. слабый контроль со стороны руководства и соответствующих служб за установленным порядком защиты информации.
3. Основными направлениями деятельности по пресечению разглашения охраняемых сведений являются правовые и организационные меры по повышению ответственности сотрудников к соблюдению установленных мер и требований по защите конфиденциальной информации.

Глава 5 ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ [^]

Защита информации от утечки по техническим каналам — это комплекс организационных, организационно-технических и технических мероприятий, исключающих или ослабляющих бесконтрольный выход конфиденциальной информации за пределы контролируемой зоны.

Постулаты

1. Безопасных технических средств нет.
2. Источниками образования технических каналов утечки информации являются физические преобразователи.
3. Любой электронный элемент при определенных условиях может стать источником образования канала утечки информации.
4. Любой канал утечки информации может быть обнаружен и локализован. «На каждый яд есть противоядие».
5. Канал утечки информации легче локализовать, чем обнаружить.

Определив утечку информации как бесконтрольный выход охраняемых сведений за пределы организации или круга лиц, которым они были доверены по службе или стали известны в процессе работы, рассмотрим, что же способствует этому и по каким каналам осуществляется такая утечка.

В основе утечки лежит неконтролируемый перенос конфиденциальной информации посредством акустических, световых, электромагнитных, радиационных и других полей и материальных объектов.

Что касается причин и условий утечки информации, то они, при всех своих различиях, имеют много общего.

Причины связаны, как правило, с несовершенством норм по сохранению информации, а также нарушением этих норм (в том числе и несовершенных), отступлением от правил обращения с соответствующими документами, техническими средствами, образ-

цами продукции и другими материалами, содержащими конфиденциальную информацию

Условия включают различные факторы и обстоятельства, которые складываются в процессе научной, производственной, рекламной, издательской, отчетной, информационной и иной деятельности предприятия (организации) и создают предпосылки для утечки информации. К таким факторам и обстоятельствам могут, например, относиться:

- недостаточное знание работниками предприятия правил защиты информации и непонимание (или недопонимание) необходимости их тщательного соблюдения;
- использование не аттестованных технических средств обработки конфиденциальной информации;
- слабый контроль за соблюдением правил защиты информации правовыми, организационными и инженерно-техническими мерами;
- текучесть кадров, в том числе владеющих сведениями конфиденциального характера.

Таким образом, большая часть причин и условий, создающих предпосылки и возможность утечки конфиденциальной информации, возникает из-за недоработок руководителей предприятий и их сотрудников.

Кроме того, утечке информации способствуют:

- стихийные бедствия (шторм, ураган, смерч, землетрясение, наводнение);
- неблагоприятная внешняя среда (гроза, дождь, снег);
- катастрофы (пожар, взрывы);
- неисправности, отказы, аварии технических средств и оборудования (рис. 39).

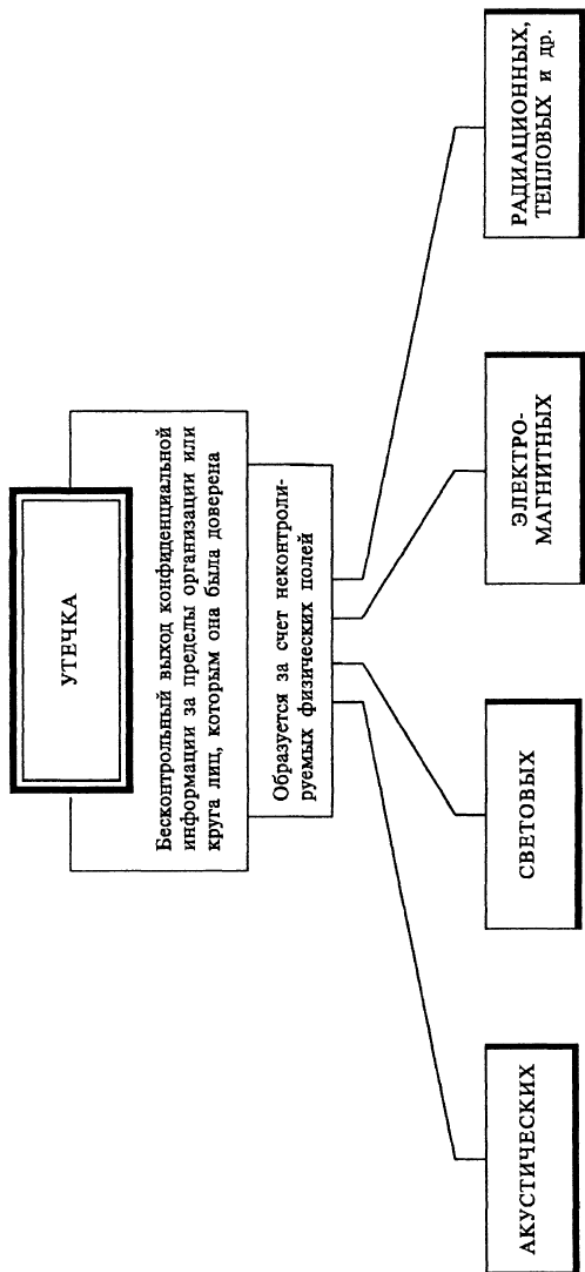


Рис. 39

5.1. Общие положения [^]

Известно, что информация вообще передается полем или веществом. Это либо акустическая волна (звук), либо электромагнитное излучение, либо лист бумаги с текстом. Но ни переданная энергия, ни посланное вещество сами по себе никакого значения не имеют, они служат лишь носителями информации. Человек не рассматривается как носитель информации. Он выступает субъектом отношений или источником.

Основываясь на этом, можно утверждать, что по физической природе возможны следующие средства переноса информации:

- световые лучи;
- звуковые волны;
- электромагнитные волны;
- материалы и вещества.

Иной возможности для переноса информации в природе не существует (рис. 40).

Используя в своих интересах те или иные физические поля, человек создает определенную систему передачи информации друг другу. Такие системы принято называть системами связи. Любая система связи (система передачи информации) состоит из источника информации, передатчика, канала передачи информации, приемника и получателя сведений. Эти системы используются в повседневной практике в соответствии со своим предназначением и являются официальными средствами передачи информации, работа которых контролируется с целью обеспечения надежной, достоверной и безопасной передачи информации, исключающей неправомерный доступ к ней со стороны конкурентов. Однако существуют определенные условия, при которых возможно образование системы передачи информации из одной точки в другую независимо от желания объекта и источника. При этом, естественно, такой канал в явном виде не должен себя проявлять. По аналогии с каналом передачи информации такой канал называют каналом утечки информации. Он также состоит из источника сигнала, физической среды его распространения и приемной

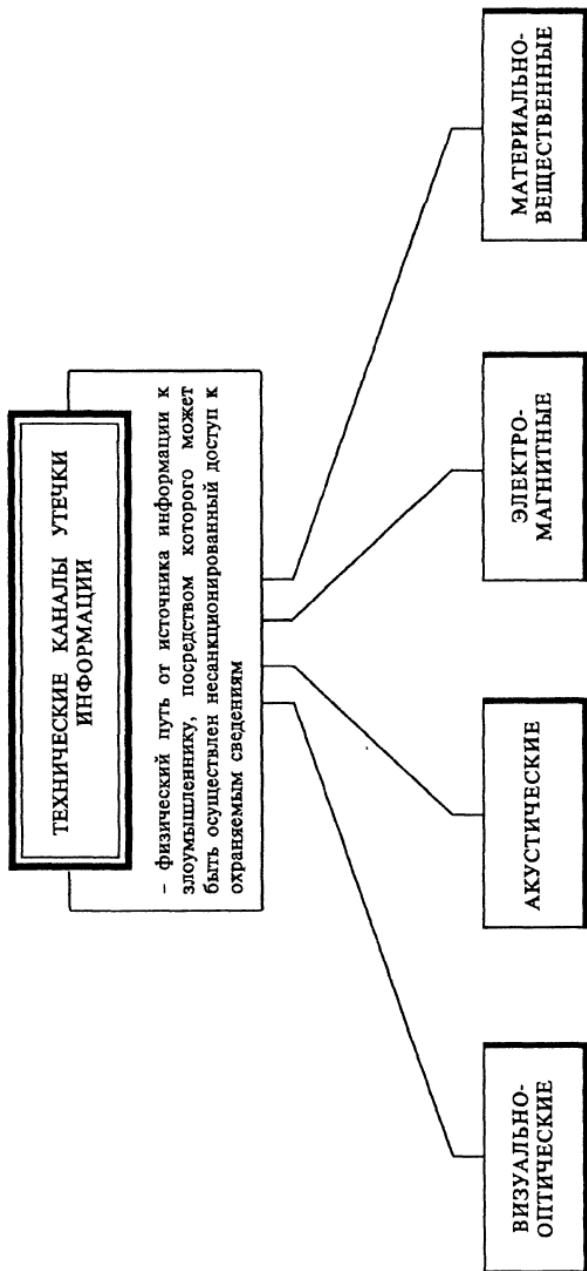


Рис. 40

паратуры на стороне злоумышленника. Движение информации в таком канале осуществляется только в одну сторону — от источника к злоумышленнику. На рис. 41 приведена структура канала утечки информации.

СТРУКТУРА КАНАЛА УТЕЧКИ ИНФОРМАЦИИ



Рис. 41

Под каналом утечки информации будем понимать физический путь от источника конфиденциальной информации к злоумышленнику, по которому возможна утечка или несанкционированное получение охраняемых сведений. Для возникновения (образования, установления) канала утечки информации необходимы определенные пространственные, энергетические и временные условия, а также соответствующие средства восприятия и фиксации информации на стороне злоумышленника.

Применительно к практике с учетом физической природы образования каналы утечки информации можно разделить на следующие группы:

- визуально-оптические;
- акустические (включая и акустико-преобразовательные);
- электромагнитные (включая магнитные и электрические);
- материально-вещественные (бумага, фото, магнитные носители, производственные отходы различного вида — твердые, жидкие, газообразные).

Каждому виду каналов утечки информации свойственны свои специфические особенности.

Визуально-оптические каналы — это, как правило, непосредственное или удаленное (в том числе и телевизионное) наблюдение. Переносчиком информации выступает свет, испускаемый источником конфиденциальной информации или отраженный от него в видимом, инфракрасном и ультрафиолетовом диапазонах,

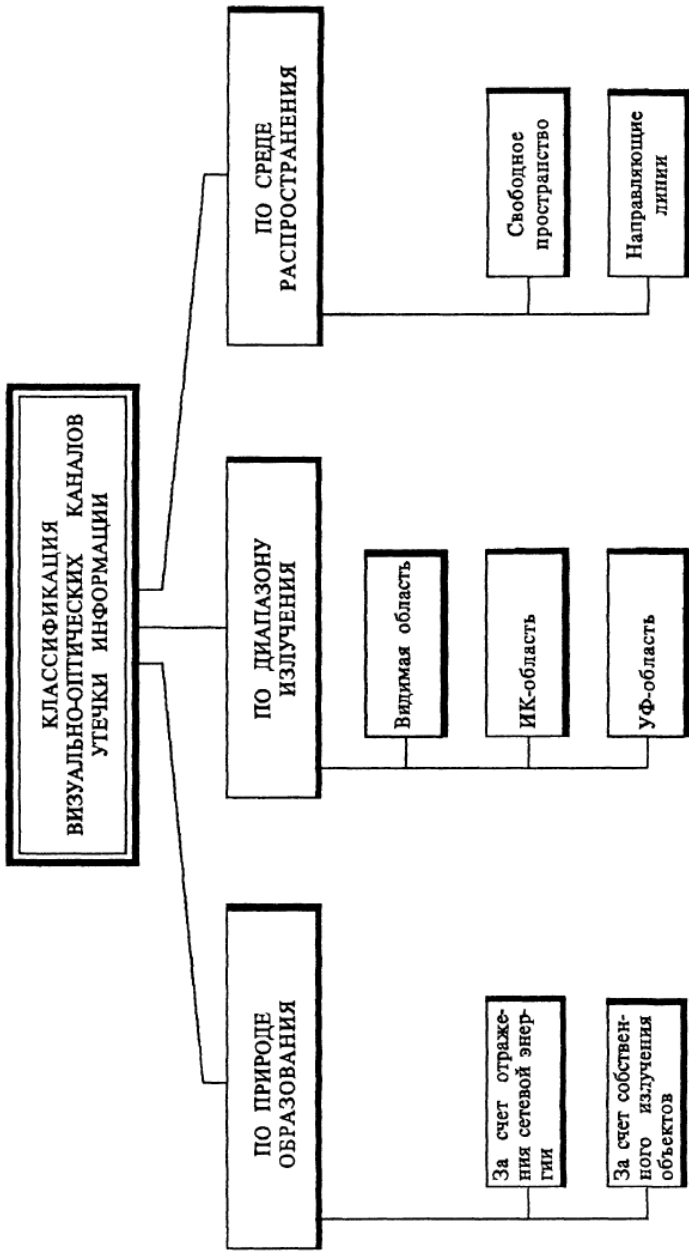


Рис. 42

Классификация визуально-оптических каналов приведена на рис. 42.

Акустические каналы. Для человека слух является вторым по информативности после зрения. По этому одним из довольно распространенных каналов утечки информации является акустический канал. В акустическом канале переносчиком информации выступает звук, лежащий в полосе ультра (более 20 000 Гц), слышимого и инфразвукового диапазонов. Диапазон звуковых частот, слышимых человеком, лежит в пределах от 16 до 20 000 Гц, и содержащихся в человеческой речи — от 100 до 6000 Гц.

Когда в воздухе распространяется акустическая волна, частицы воздуха приобретают колебательные движения, передавая колебательную энергию друг другу. Если на пути звука нет препятствия, он распространяется равномерно во все стороны. Если же на пути звуковой волны возникают какие-либо препятствия в виде перегородок, стен, окон, дверей, потолков и т. п., звуковые волны оказывают на них соответствующее давление, приводя их также в колебательный режим. Эти воздействия звуковых волн и являются одной из основных причин образования акустического канала утечки информации.

Различают определенные особенности распространения звуковых волн в зависимости от среды. Это прямое распространение звука в воздушном пространстве, распространение звука в жестких средах (структурный звук) (рис. 43). Кроме того, воздействие звукового давления на элементы конструкции зданий и помещений вызывает их вибрацию.

В свободном воздушном пространстве акустические каналы образуются в помещениях при ведении переговоров в случае открытых дверей, окон, форточек. Кроме того, такие каналы образуются системой воздушной вентиляции помещений. В этом случае образование каналов существенно зависит от геометрических размеров и формы воздуховодов, акустических характеристик фасонных элементов задвижек, воздухо-хораспределителей и подобных элементов.

Под структурным звуком понимают механические колебания в твердых средах. Механические колебания стен, перекрытий или трубопроводов, возникающие в

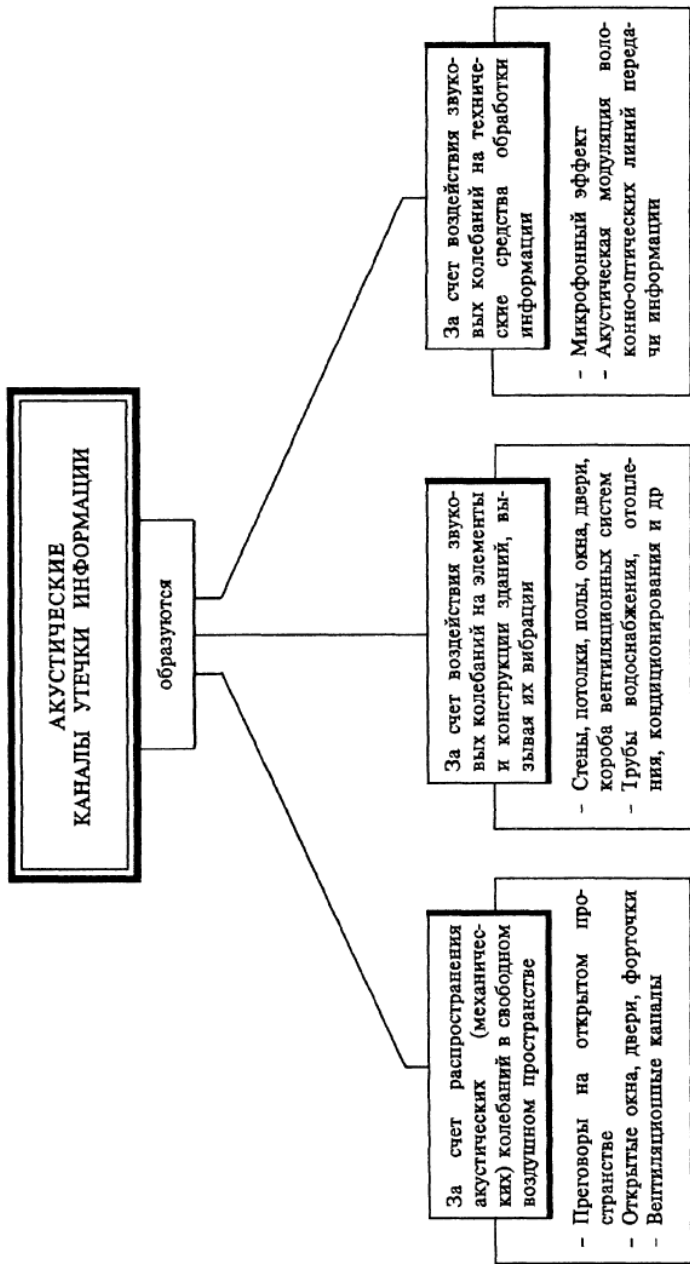


Рис 43

одном месте, передаются на значительные расстояния почти незатухая. Опасность такого канала утечки состоит в неконтролируемой дальности распространения звука.

На рис. 44 представлена схема акустических и вибрационных каналов утечки информации, наглядно показывающая, как распределяются акустические колебания и структурный звук в жестких средах, в металлических конструкциях волновода и других элементах зданий и сооружений.

Преобразовательный, а точнее, акусто-преобразовательный канал — это изменение тех или иных сигналов электронных схем под воздействием акустических полей. На практике такое явление принято называть микрофонным эффектом.

Электромагнитные каналы. Переносчиком информации являются электромагнитные волны в диапазоне от сверхдлинных с длиной волны 10 000 м (частоты менее 30 Гц) до субмиллиметровых с длиной волны 1—0,1 мм (частоты от 300 до 3000 ГГц). Каждый из этих видов электромагнитных волн обладает специфическими особенностями распространения как по дальности, так и в пространстве. Длинные волны, например, распространяются на весьма большие расстояния, миллиметровые — наоборот, на удаление лишь прямой видимости в пределах единиц и десятков километров. Кроме того, различные телефонные и иные провода и кабели связи создают вокруг себя магнитное и электрическое поля, которые также выступают элементами утечки информации за счет наводок на другие провода и элементы аппаратуры в ближней зоне их расположения.

Материально-вещественными каналами утечки информации выступают самые различные материалы в твердом, жидком и газообразном или корпускулярном (радиоактивные элементы) виде. Очень часто это различные отходы производства, бракованные изделия, черновые материалы и другое.

Очевидно, что каждый источник конфиденциальной информации может обладать в той или иной степени какой-то совокупностью каналов утечки информации (рис. 45).

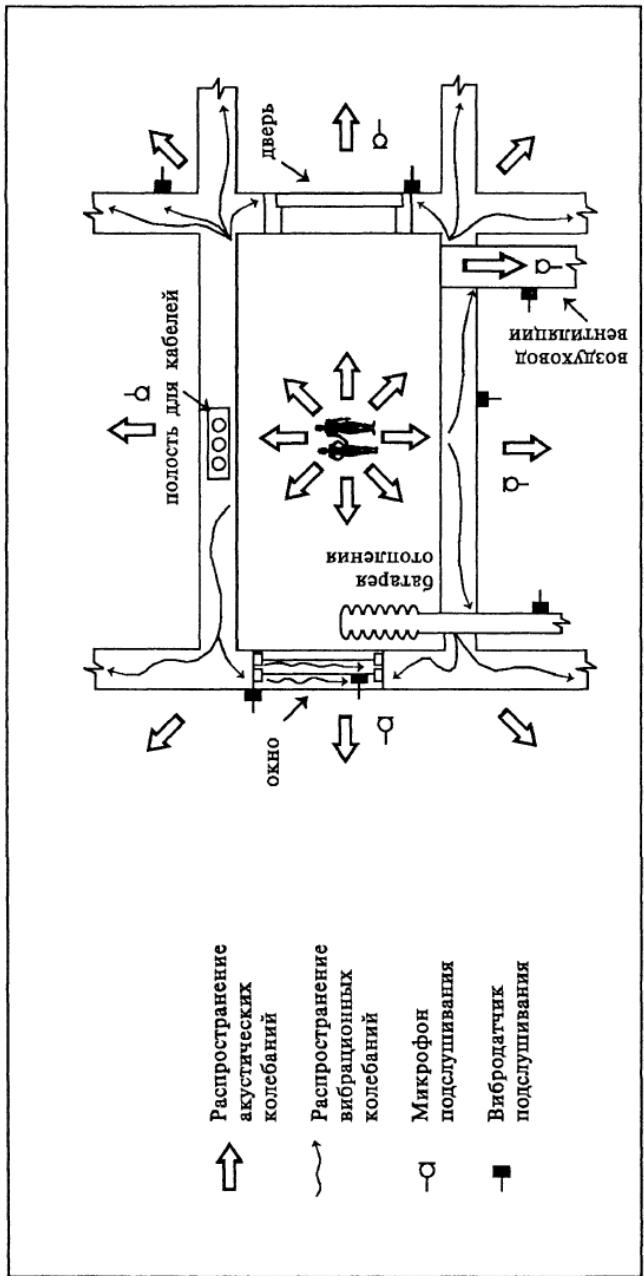


Рис. 44. Схема акустических и вибрационных каналов утечки

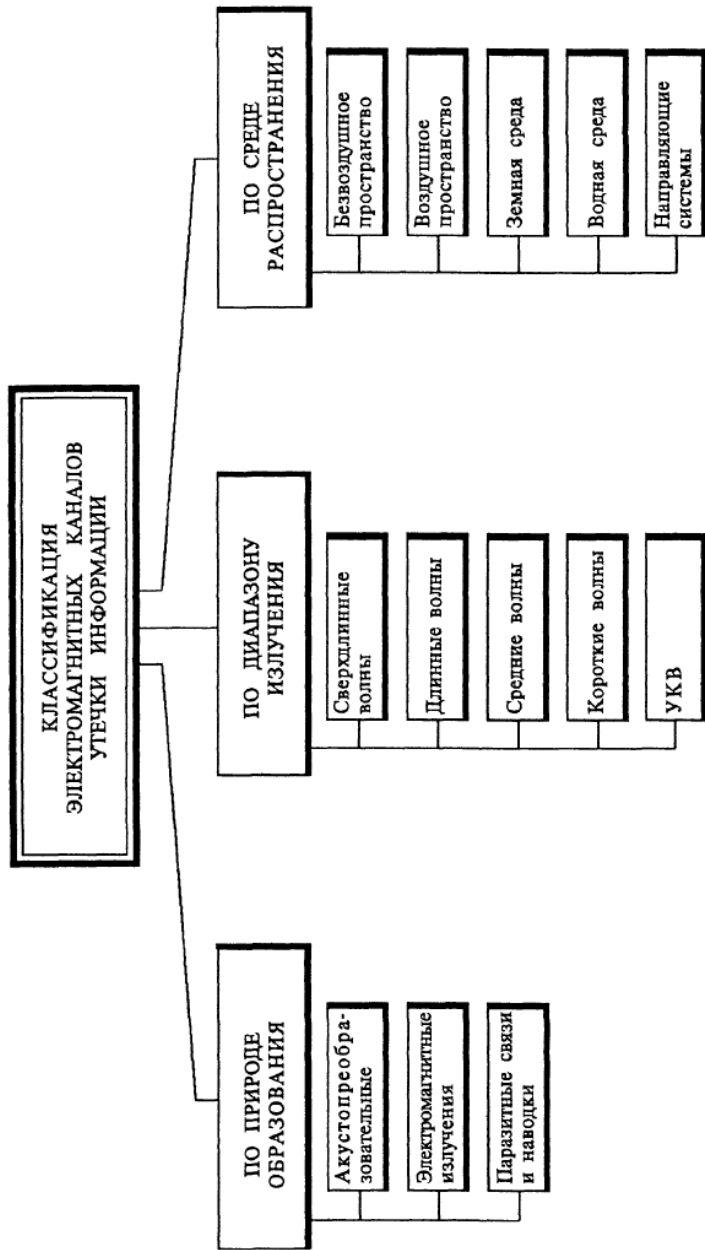


Рис. 45

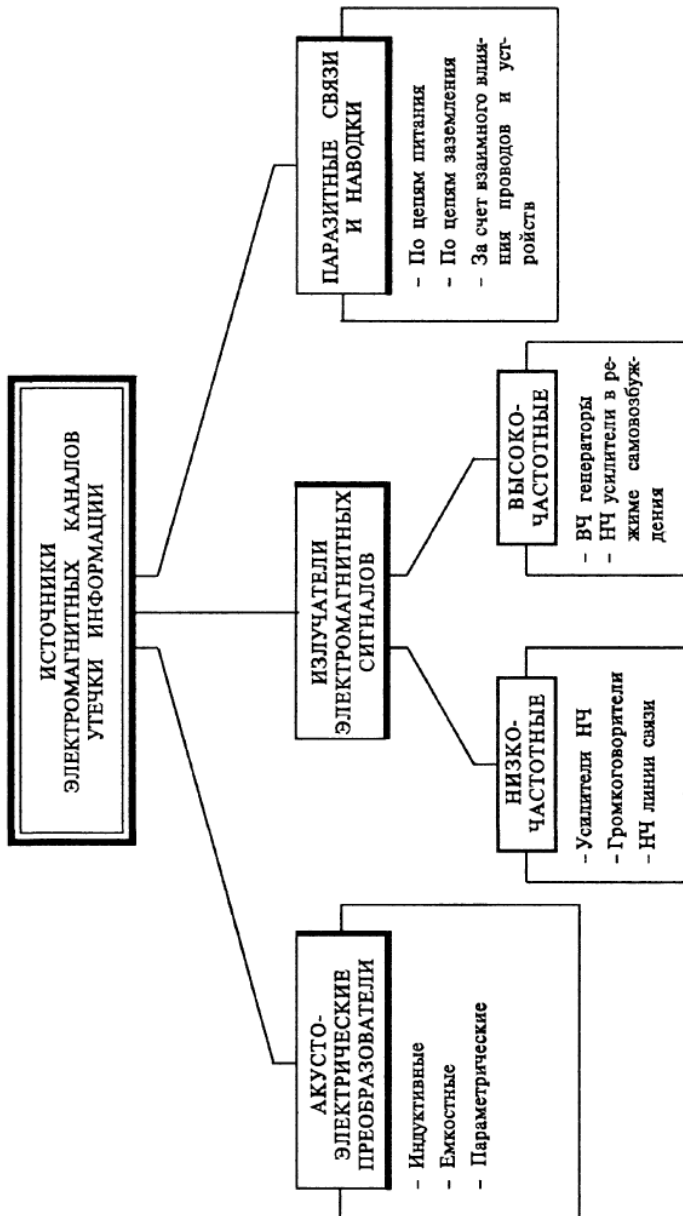


Рис. 46

Широкое использование самых различных технических

средств обеспечения производственной и научной деятельности и автоматизированной обработки привело к появлению группы каналов утечки информации, которые стали называться техническими. Переносчиками информации в них выступают побочные электромагнитные излучения и наводки различного происхождения: акусто-преобразовательные, излучательные и паразитные связи и наводки. Побочные электромагнитные излучения и наводки (ПЭМИН) присущи любым электронным устройствам, системам, изделиям по самой природе проявления. О том, что ПЭМИН могут образовать канал утечки информации, известно давно. Интересный факт имел место в 1884 году в Лондоне. Было обнаружено, что в телефонных аппаратах по улице Грей-Стоун-Роуд прослушиваются какие-то телеграфные передачи. Проверка показала, что причиной этих сигналов были заложенные неглубоко под землей телеграфные провода, идущие на большом протяжении параллельно телефонным проводам. Можно считать, что это был первый намек на возможность неконтролируемого получения информации (утечки) за счет побочных излучений.

Современная предпринимательская деятельность немислима без разнообразных технических средств и систем, предназначенных для приема, передачи и обработки информации. Физические процессы, происходящие в таких устройствах при их функционировании, создают в окружающем пространстве подобные акустические и электромагнитные излучения, которые в той или иной степени связаны с обрабатываемой информацией.

Физические явления, лежащие в основе появления опасных излучений, имеют различный характер, тем не менее в общем виде утечка информации за счет подобных излучений может рассматриваться как непреднамеренная передача охраняемой информации по некоторой «побочной» системе связи.

Следует отметить, что технические средства и системы могут не только непосредственно излучать в пространство сигналы, содержащие обрабатываемую информацию, но и улавливать за счет своих микрофонных, или антенных свойств акустические или магнитные (электромагнитные) излучения, преобразовывать их в электрические сигналы и передавать по своим линиям связи, как правило, бесконтрольно, что в еще большей степени повышает опасность утечки информации.

Отдельные технические средства имеют в своем составе помимо подобных «микрофонов» и «антенн» высокочастотные или импульсные генераторы, излучения которых могут быть

промодулированными различными сигналами, содержащими конфиденциальную информацию.

Опасный «микрофонный эффект» (образование паразитного электрического сигнала) возникает в некоторых телефонных аппаратах даже при положенной микрофонной трубке. Электромагнитные излучения могут образовываться и при самовозбуждении на радиочастотах звуковоспроизводящей и звукоусилительной аппаратуры.

Анализ условий и причин образования источников появления ПЭМИН показал, что для этого имеется ряд причин и условий. К ним можно отнести несовершенство схемных решений, принятых для данной категории технических средств, и эксплуатационный износ элементов изделия (рис. 47).

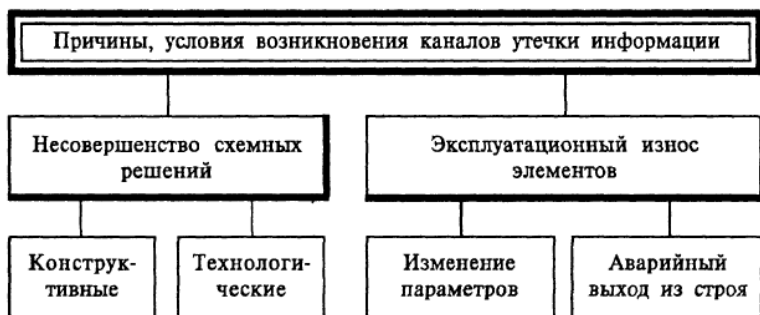


Рис. 47. Причины возникновения технических каналов утечки информации

Защита информации от утечки по техническим каналам в общем плане сводится к следующим действиям:

1. Своевременному определению возможных каналов утечки информации.

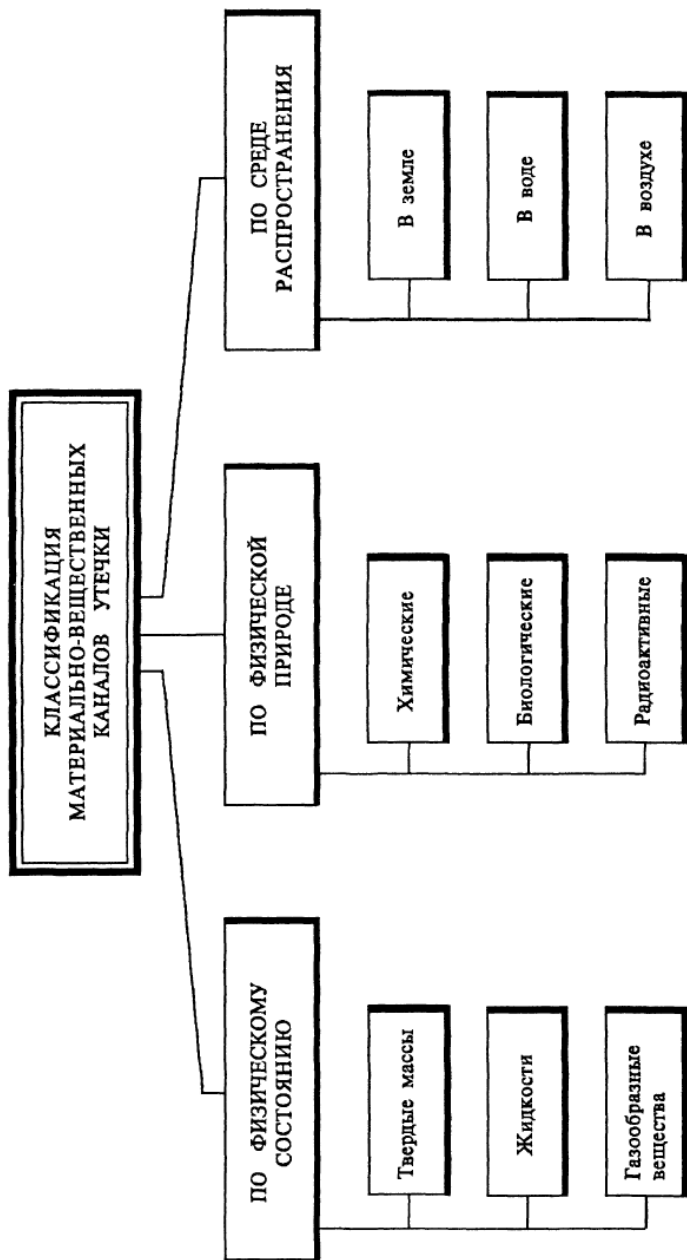


Рис. 48

2. Определению энергетических характеристик канала утечки на границе контролируемой зоны (территории, кабинета).
3. Оценке возможности средств злоумышленников обеспечить контроль этих каналов.
4. Обеспечению исключения или ослабления энергетики каналов утечки соответствующими организационными, организационно-техническими или техническими мерами и средствами.

5.2. Защита информации от утечки по визуальным оптическим каналам [^]

Защита информации от утечки по визуальном-оптическому каналу — это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет распространения световой энергии.

5.2.1. Общие положения [^]

Человек видит окружающий его мир и предметы за счет отраженного от них света либо за счет их собственного излучения.

Наиболее привычным для человека носителем информации об объектах его интересов является видимое человеческим глазом излучение. С помощью зрительной системы человек получает наибольший (до 90%) объем информации из внешнего мира. Соседние участки видимого спектра — инфракрасный и ультрафиолетовый — также несут существенную информацию об окружающих предметах, но она не может быть воспринята человеческим глазом непосредственно. Для этих целей используются различного рода преобразователи невидимого изображения в видимое — визуализация невидимых изображений.

Окружающий нас мир освещается естественным светом (Солнце, Луна, звезды) и искусственным освещением. Возможность наблюдения объектов определяется величиной падающего потока света (освещенность), отраженного от объекта света (отражающие свойства) и контрастом объекта на фоне окружающих его предметов.

В дневное время, когда освещенность создается светом Солнца, глаз человека обладает наибольшей цветовой и

контрастной чувствительностью. В сумерки, когда солнечный диск постепенно уходит за линию горизонта, освещенность падает в зависимости от глубины погружения Солнца. Уменьшение освещенности вызывает ухудшение работы зрения, а следовательно, сокращение дальности и ухудшение цветоразличия. Эти физические особенности необходимо учитывать при защите информации от утечки по визуально-оптическим каналам.

5.2.2. Средства и способы защиты [^]

С целью защиты информации от утечки по визуально-оптическому каналу рекомендуется:

- располагать объекты защиты так, чтобы исключить отражение света в стороны возможного расположения злоумышленника (пространственные ограждения);
- уменьшить отражательные свойства объекта защиты;
- уменьшить освещенность объекта защиты (энергетические ограничения);
- использовать средства преграждения или значительного ослабления отраженного света: ширмы, экраны, шторы, ставни, темные стекла и другие преграждающие среды, преграды;
- применять средства маскирования, имитации и другие с целью защиты и введения в заблуждение злоумышленника;
- использовать средства пассивной и активной защиты источника от неконтролируемого распространения отражательного или излученного света и других излучений;
- осуществлять маскировку объектов защиты, варьируя отражательными свойствами и контрастом фона;
- применять маскирующие средства сокрытия объектов можно в виде аэрозольных завес и маскирующих сеток, красок, укрытий.

В качестве оперативных средств сокрытия находят широкое применение аэрозольные завесы. Это взвешенные в газообразной среде мельчайшие частицы различных веществ, которые в зависимости от размеров и агрегатного сочетания образуют дым, копоть, туман. Они преграждают распространение отраженного от объекта защиты света. Хорошими светопоглощающими свойствами обладают дымообразующие вещества.

Аэрозольные образования в виде маскирующих завес

обеспечивают индивидуальную или групповую защиту объектов и техники, в том числе и выпускаемую продукцию.

5.3. Защита информации от утечки по акустическим каналам [^]

Защита информации от утечки по акустическому каналу — это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет акустических полей.

5.3.1. Общие положения [^]

Основными мероприятиями в этом виде защиты выступают организационные и организационно-технические меры.

Организационные меры предполагают проведение архитектурно-планировочных, пространственных и режимных мероприятий, а организационно-технические — пассивных (звукоизоляция, звукопоглощение) и активных (звукоподавление) мероприятий. Не исключается проведение и технических мероприятий за счет применения специальных защищенных средств ведения конфиденциальных переговоров (рис. 49).

Архитектурно-планировочные меры предусматривают предъявление определенных требований на этапе проектирования зданий и помещений или их реконструкцию и приспособление с целью исключения или ослабления неконтролируемого распространения звуковых полей непосредственно в воздушном пространстве или в строительных конструкциях в виде 1/10 структурного звука. Эти требования могут предусматривать как выбор расположения помещений в про-

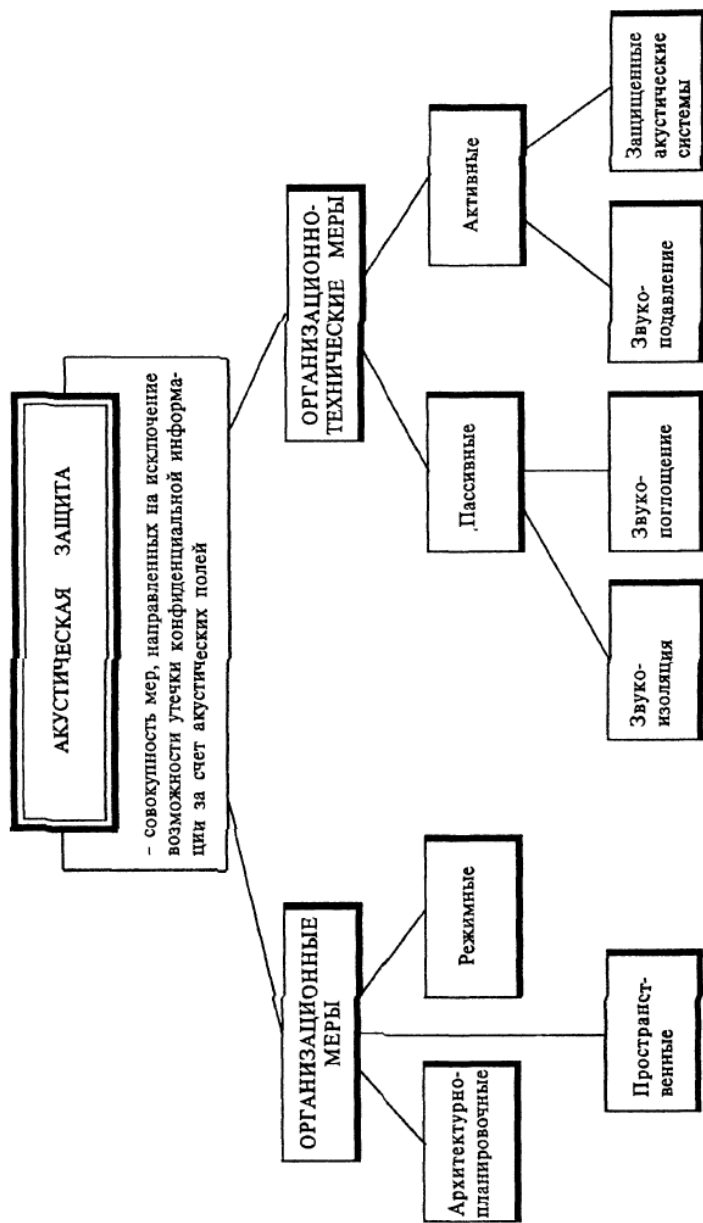


Рис. 49

странственном плане, так и их оборудование необходимы для акустической безопасности элементами, исключаящими прямое или отраженное в сторону возможного расположения злоумышленника распространение звука. В этих целях двери оборудуются тамбурами, окна ориентируются в сторону охраняемой (контролируемой) от присутствия посторонних лиц территории и пр.

Режимные меры предусматривают строгий контроль пребывания в контролируемой зоне сотрудников и посетителей.

Организационно-технические меры предусматривают использование звукопоглощающих средств. Пористые и мягкие материалы типа ваты, ворсистые ковры, пенобетон, пористая сухая штукатурка являются хорошими звукоизолирующими и звукопоглощающими материалами — в них очень много поверхностей раздела между воздухом и твердым телом, что приводит к многократному отражению и поглощению звуковых колебаний.

Для облицовки поверхностей стен и потолков широко используются специальные герметические акустические панели, изготавливаемые из стекловаты высокой плотности и различной толщины (от 12 до 50 мм). Такие панели обеспечивают поглощение звука и исключают его распространение в стеновых конструкциях. Степень звукопоглощения α , отражения и пропускания звука преградами характеризуется коэффициентами звукопоглощения, отражения β , пропускания τ .

Степень отражения и поглощения звуковой энергии определяется частотой звука и материалом отражающих (поглощающих) конструкций (пористостью, конфигурацией, толщиной).

Устраивать звукоизолирующие покрытия стен целесообразно в небольших по объему помещениях, так как в больших помещениях звуковая энергия максимально поглощается, еще не достигнув стен. Известно, что воздушная среда обладает некоторой звукопоглощающей способностью и сила звука убывает в воздухе пропорционально квадрату расстояния от источника.

Внутри помещения уровень громкости звучит выше, чем на открытом пространстве, из-за многократных отражений от различных поверхностей, обеспечивающих продолжение звучания даже после прекращения работы источника звука (реверберация). Уровень реверберации зависит от степени звукопоглощения.

Величина звукопоглощения A определяется коэффициентом

звукопоглощения α и размерами звукопоглощающей поверхности:

$$A = \sum \alpha * S.$$

Значения коэффициентов звукопоглощения различных материалов известны. Для обычных пористых материалов — войлока, ваты, пористой штукатурки — оно колеблется в пределах $\alpha = 0,2 — 0,8$. Кирпич и бетон почти не поглощают звук ($\alpha = 0,01 — 0,03$).

Степень ослабления звука при применении звукопоглощающих покрытий определяется в децибелах.

Например, при обработке кирпичных стен ($\alpha = 0,03$) пористой штукатуркой ($\alpha = 0,3$) звуковое давление в помещении ослабляется на 10 дБ ($8 = 10 \lg \Delta$).

5.3.2. Способы и средства защиты [^]

Для определения эффективности защиты звукоизоляции используются шумомеры. Шумомер — это измерительный прибор, который преобразует колебания звукового давления в показания, соответствующие уровню звукового давления. В сфере акустической защиты речи используются аналоговые шумомеры (рис. 50).

По точности показаний шумомеры подразделяются на четыре класса. Шумомеры нулевого класса служат для лабораторных измерений, первого — для натуральных измерений, второго — для общих целей; шумомеры третьего класса используются для ориентированных измерений. На практике для оценки степени защищенности акустических каналов используются шумомеры второго класса, реже — первого.

Измерения акустической защищенности реализуются методом образцового источника звука. Образцовым называется источник с заранее известным уровнем мощности на определенной частоте (частотах),

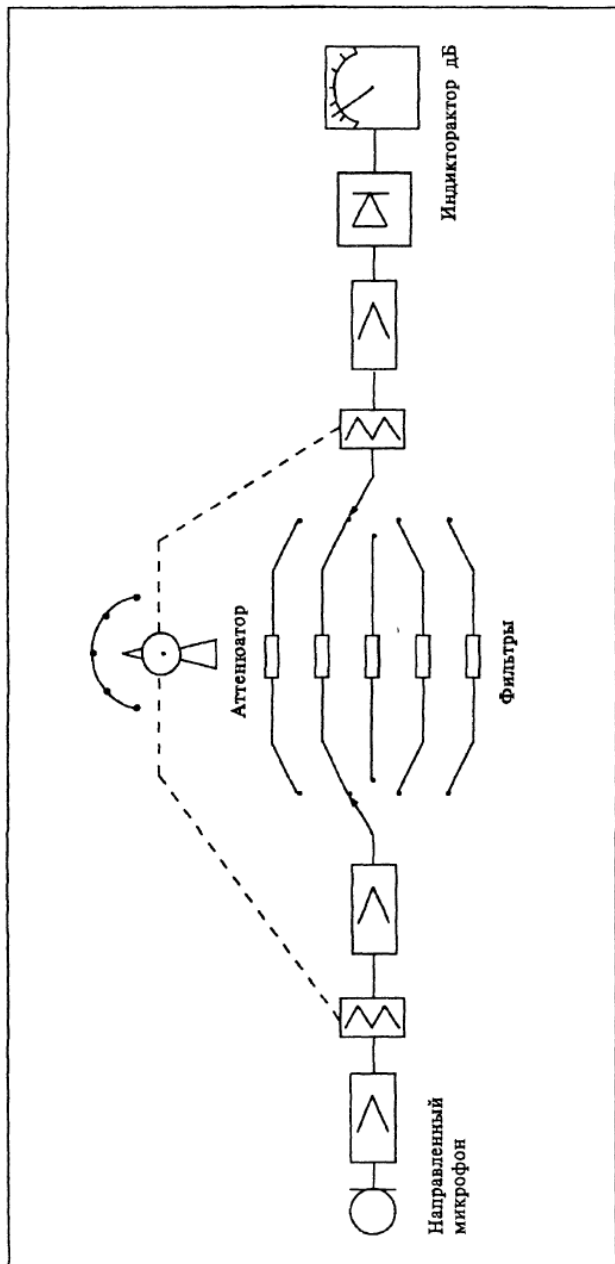


Рис. 50. Блок-схема аналогового шумомера

Выбирается в качестве такого источника магнитофон с записанным на пленку сигналом на частотах 500 Гц и 1000 Гц, модулированным синусоидальным сигналом в 100—120 Гц. Имея образцовый источник звука и шумомер, можно определить поглощающие возможности помещения, как показано на рис. 51.

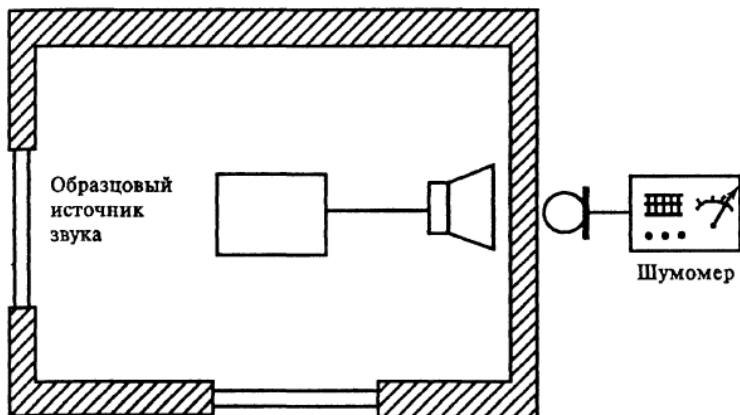


Рис. 51

Величина акустического давления образцового источника звука известна. Принятый с другой стороны стены сигнал замерен по показаниям шумомера. Разница между показателями и дает коэффициент поглощения.

В зависимости от категории выделенного помещения эффективность звукоизоляции должна быть разной. Рекомендуются следующие нормативы поглощения на частотах 500 и 1000 Гц соответственно (табл. 4).

Таблица 4

| Частота сигнала (Гц) | Категории помещений (дБ) кэфф. поглощения | | |
|----------------------|---|----|-----|
| | I | II | III |
| 500 | 53 | 48 | 43 |
| 1000 | 56 | 51 | 46 |

Для проведения оценочных измерений защищенности помещений от утечки по акустическим и вибрационным каналам используются так называемые электронные стетоскопы. Они позволяют прослушивать ведущиеся в помещении переговоры

через стены, полы, потолки, системы отопления, водоснабжения, вентиляционные коммуникации и другие металлоконструкции. В качестве чувствительного элемента в них используется датчик, преобразующий механические колебания звука в электрический сигнал. Чувствительность стетоскопов колеблется от 0,3 до 1,5 в/дБ. При уровне звукового давления 34 — 60 дБ, соответствующем средней громкости разговора, современные стетоскопы позволяют прослушивать помещения через стены и другие ограждающие конструкции толщиной до 1,5 м. После проверки с помощью такого стетоскопа возможных каналов утечки принимаются меры по их защите. В качестве примера можно привести электронный стетоскоп «Бриз» («Элерон»). Рабочие диапазоны частот— 300 — 4000 Гц, питание автономное. Предназначен для выявления вибрационно-акустических каналов утечки информации, циркулирующей в контролируемом помещении, через ограждения конструкции или коммуникации, а также для контроля эффективности средств защиты информации.

В тех случаях, когда пассивные меры не обеспечивают необходимого уровня безопасности, используются активные средства. К активным средствам относятся генераторы шума — технические устройства, вырабатывающие шумоподобные электронные сигналы. Эти сигналы подаются на соответствующие датчики акустического или вибрационного преобразования. Акустические датчики предназначены для создания акустического шума в помещениях или вне их, а вибрационные — для маскирующего шума в ограждающих конструкциях. Вибрационные датчики приклеиваются к защищаемым конструкциям, создавая в них звуковые колебания.

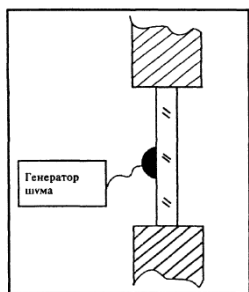


Рис. 52. Защита окна посредством генератора шума

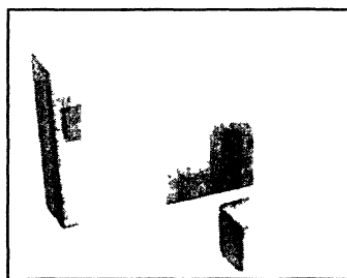


Рис 53

В качестве примера генераторов шума можно привести систему виброакустического зашумления «Заслон» («Маском»). Система позволяет защитить до 10 условных поверхностей, имеет автоматическое включение вибропреобразователей при появлении акустического сигнала. Эффективная шумовая полоса частот 100 — 6000 Гц (рис. 53). На рис. 54 приведен пример размещения в охраняемом помещении системы акустических и вибрационных датчиков.

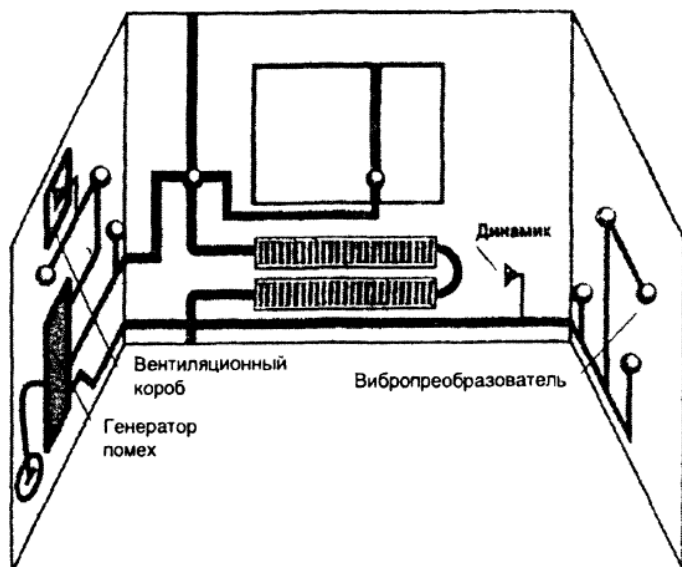


Рис 54. Вариант размещения датчиков акустической защиты

Современные генераторы шума обладают эффективной полосой частот в пределах от 100 — 200 Гц до 5000 — 6000 Гц. Отдельные типы генераторов имеют полосу частот до 10 000 Гц. Число подключаемых к одному генератору датчиков различно — от 1 — 2 до 20 — 30 штук. Это определяется назначением и конструктивным исполнением генератора.

Используемые на практике генераторы шума позволяют защищать информацию от утечки через стены, потолки, полы, окна, двери, трубы, вентиляционные коммуникации и другие конструкции с достаточно высокой степенью надежности. В

таблице 5 приведены технические характеристики акустических генераторов.

Таблица 5

| Тип | Шумовая полоса (Гц) | Излучатели | | Количество |
|-----------|---------------------|--------------|--------------|------------|
| | | Вибрационные | Акустические | |
| «Заслон» | 100-6000 | 6 | 2 | до 10 |
| ANG-2000 | 250-5000 | - | - | - |
| WNG-033 | 100-12000 | - | - | до 18 |
| «Кабинет» | 100-6000 | - | - | до 30 |

Итак, защита от утечки по акустическим каналам реализуется:

- применением звукопоглощающих облицовок, специальных дополнительных тамбуров дверных проемов, двойных оконных переплетов;
- использованием средств акустического шумления объемов и поверхностей;
- закрытием вентиляционных каналов, систем ввода в помещения отопления, электропитания, телефонных и радиосвязей;
- использованием специальных аттестованных помещений, исключающих появление каналов утечки информации.

5.4. Защита информации от утечки по электромагнитным каналам [^]

Защита информации от утечки по электромагнитным каналам — это комплекс мероприятий, исключающих или ослабляющих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны за счет электромагнитных полей побочного характера и наводок.

Известны следующие электромагнитные каналы утечки информации:

- микрофонный эффект элементов электронных схем;
- электромагнитное излучение низкой и высокой частоты;
- возникновение паразитной генерации усилителей различного назначения;
- цепи питания и цепи заземления электронных схем;

- взаимное влияние проводов и линий связи;
- высокочастотное навязывание;
- волоконно-оптические системы.

Для защиты информации от утечки по электромагнитным каналам применяются как общие методы защиты от утечки, так и специфические — именно для этого вида каналов. Кроме того, защитные действия можно классифицировать на конструкторско-технологические решения, ориентированные на исключение возможности возникновения таких каналов, и эксплуатационные, связанные с обеспечением условий использования тех или иных технических средств в условиях производственной и трудовой деятельности.

Конструкторско-технологические мероприятия по локализации возможности образования условий возникновения каналов утечки информации за счет побочных электромагнитных излучений и наводок в технических средствах обработки и передачи информации сводятся к рациональным конструкторско-технологическим решениям, к числу которых относятся:

- экранирование элементов и узлов аппаратуры;
- ослабление электромагнитной, емкостной, индуктивной связи между элементами и токонесущими проводами;
- фильтрация сигналов в цепях питания и заземления и другие меры, связанные с использованием ограничителей, развязывающих цепей, систем взаимной компенсации, ослабителей по ослаблению или уничтожению ПЭМИН (рис. 55).

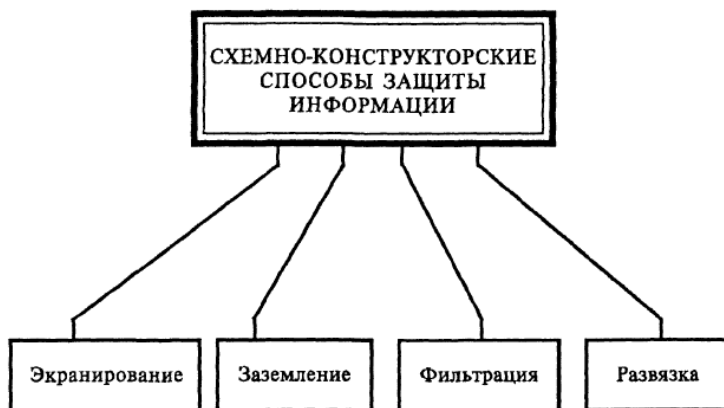


Рис. 55

Экранирование позволяет защитить их от нежелательных воздействий акустических и электромагнитных сигналов и излучений собственных электромагнитных полей, а также ослабить (или исключить) паразитное влияние внешних излучений. Экранирование бывает электростатическое, магнитостатическое и электромагнитное.

Электростатическое экранирование заключается в замыкании силовых линий электростатического поля источника на поверхность экрана и отводе наведенных зарядов на массу и на землю. Такое экранирование эффективно для устранения емкостных паразитных связей. Экранирующий эффект максимален на постоянном токе и с повышением частоты снижается.

Магнитостатическое экранирование основано на замыкании силовых линий магнитного поля источника в толще экрана, обладающего малым магнитным сопротивлением для постоянного тока и в области низких частот.

С повышением частоты сигнала применяется исключительно электромагнитное экранирование. Действие электромагнитного экрана основано на том, что высокочастотное электромагнитное поле ослабляется им же созданным (благодаря образующимся в толще экрана вихревым токам) полем обратного направления.

Если расстояние между экранирующими цепями, проводями, приборами составляет 10% от четверти длины волны, то можно считать, что электромагнитные связи этих цепей осуществляются за счет обычных электрических и магнитных полей, а не в результате переноса энергии в пространстве с помощью электромагнитных волн. Это дает возможность отдельно рассматривать экранирование электрических и магнитных полей, что очень важно, так как на практике преобладает какое-либо одно из полей и подавлять другое нет необходимости.

Заземление и металлизация аппаратуры и ее элементов служат надежным средством отвода наведенных сигналов на землю, ослабления паразитных связей и наводок между отдельными цепями.

Фильтры различного назначения служат для подавления или ослабления сигналов при их возникновении или распространении, а также для защиты систем питания аппаратуры обработки информации. Для этих же целей могут применяться и другие технологические решения.

Эксплуатационные меры ориентированы на выбор мест установки технических средств с учетом особенностей их

электромагнитных полей с таким расчетом, чтобы исключить их выход за пределы контролируемой зоны. В этих целях возможно осуществлять экранирование помещений, в которых находятся средства с большим уровнем побочных электромагнитных излучений (ПЭМИ).

5.4.1. Защита от утечки за счет микрофонного эффекта [^]

Акустическая энергия, возникающая при разговоре, вызывает соответствующие колебания элементов электронной аппаратуры, что в свою очередь приводит к появлению электромагнитного излучения или электрического тока. Наиболее чувствительными элементами электронной аппаратуры к акустическим воздействиям являются катушки индуктивности, конденсаторы переменной емкости, пьезо- и оптические преобразователи.

Там, где имеются такие элементы, возможно появление микрофонного эффекта. Известно, что микрофонным эффектом обладают отдельные типы телефонных аппаратов, вторичные электрические часы системы часофикации, громкоговорители (динамики) систем радиофикации и громкоговорящей связи и другие виды технических и электронных средств обеспечения производственной и трудовой деятельности.

Защита телефонного аппарата от утечки информации за счет микрофонного эффекта может быть обеспечена организационными или техническими мерами.

Организационные меры могут быть следующие:

- выключить телефонный аппарат из розетки. Этим просто исключается источник образования микрофонного эффекта;
- заменить аппарат на защищенный (выпускаются Пермским телефонным заводом).

Технические меры сводятся к включению в телефонную линию специальных устройств локализации микрофонного эффекта.

Так, источником возникновения микрофонного эффекта телефонного аппарата является электромеханический звонок колокольного типа. Под воздействием на него акустических колебаний на выходе его катушки возникает ЭДС микрофонного эффекта (Емэ). В качестве защитных мер используются схемы подавления этой ЭДС. На рис. 56 приведена одна из возможных

схем подавления Емэ звонковой цепи ТА.

В звонковую цепь включаются два диода, образующие схему подавления Емэ. Для малых значений Емэ такая схема представляет собой большое сопротивление, тогда как для речевого сигнала, значительно большего по величине, схема открывается и речевой сигнал свободно проходит в линию. По существу, эта схема выполняет роль автоматического клапана: малую ЭДС блокирует, а речевой сигнал разговора абонента пропускает.

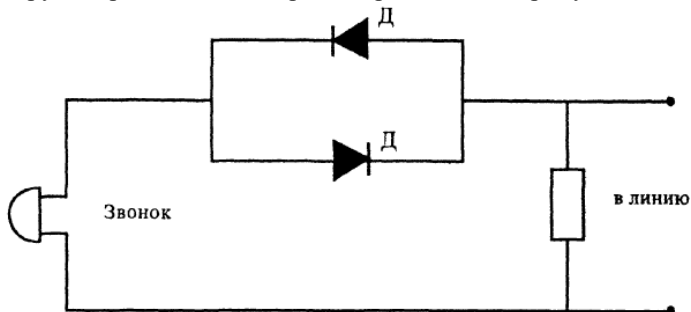


Рис. 56. Схема подавления ЭДС микрофонного эффекта звонковой цепи ТА

Находят применение и более сложные схемы (рис. 57).

Основное отличие этой схемы от предыдущей заключается в использовании двух пар диодов и фильтра высоких частот.

Обе рассмотренные схемы предотвращают возможность образования утечки информации за счет микрофонного эффекта телефонного аппарата с положенной на рычаг телефонной трубкой.

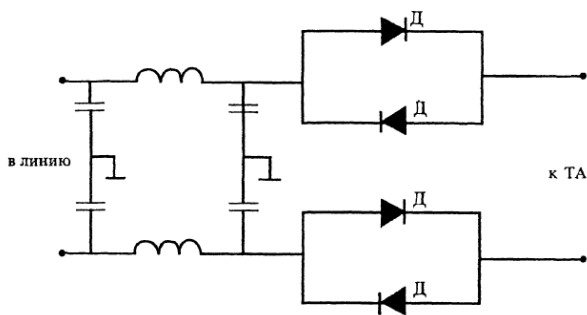


Рис. 57

Схемы подавления микрофонного эффекта исполняются в виде различных по конструкции аппаратных решений. В последнее время такие схемы стали выполняться в виде телефонной розетки, что позволяет скрывать их наличие от «любопытных» глаз.

Защита абонентского громкоговорителя радиовещательной сети или сети *диспетчерского вещания* осуществляется включением в разрыв сигнальной линии специального буферного усилителя, нагрузкой которого является однопрограммный абонентский громкоговоритель (динамик) (рис. 58).

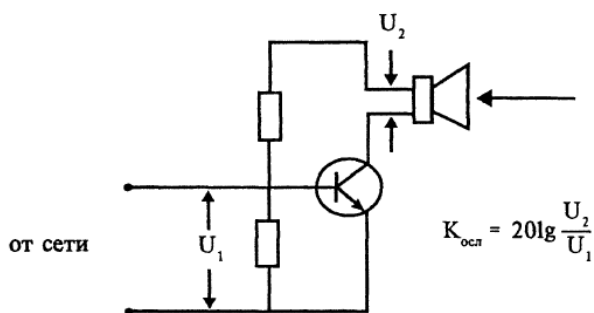


Рис. 58. Вариант буферного усилителя

Такой усилитель обеспечивает ослабление Емэ на выходе громкоговорителя порядка 120 дБ. При таком подавлении говорить перед громкоговорителем, по существу, можно с любой громкостью.

Для трехпрограммных громкоговорителей такое устройство необходимо только для низкочастотного (прямого) канала вещания, для остальных (высокочастотных) роль буфера будет выполнять усилитель преобразователя.

Блокирование канала утечки информации за счет микрофонного эффекта вторичных электро часов системы централизованной часофикации осуществляется с помощью фильтров звуковых частот, обладающих очень сильным ослаблением частот в диапазоне 700 — 3400 Гц. Как правило, стремятся использовать фильтры с коэффициентом ослабления не менее 120 дБ.

Из вышеизложенного можно заключить, что микрофонный эффект присущ самым различным техническим средствам. И

прежде чем приступить к использованию защитных мер, очевидно, следует как-то узнать, имеется ли в данном конкретном устройстве этот самый эффект.

Испытания и исследование технических средств на наличие в них микрофонного эффекта проводится на специальных испытательных стендах с использованием высококачественной испытательной аппаратуры. В качестве примера комплекта испытательной аппаратуры можно рассмотреть возможности и технические характеристики одного из таких комплектов. Комплект аппаратуры используется при разработке, испытаниях и контроле качества электроакустических и электромеханических преобразователей: телефонных аппаратов, громкоговорителей, микрофонов, наушников, слуховых аппаратов и т. д.

Специальные исследования проводятся по следующей схеме (рис. 59).

Аппаратура позволяет определить передаточные характеристики исследуемых технических средств, их эквивалентные схемы, характеристики микрофонного эффекта и другие параметры; обеспечивает измерение характеристик приема, передачи и слышимости собственного микрофона, а также обратные потери, шум и искажения.

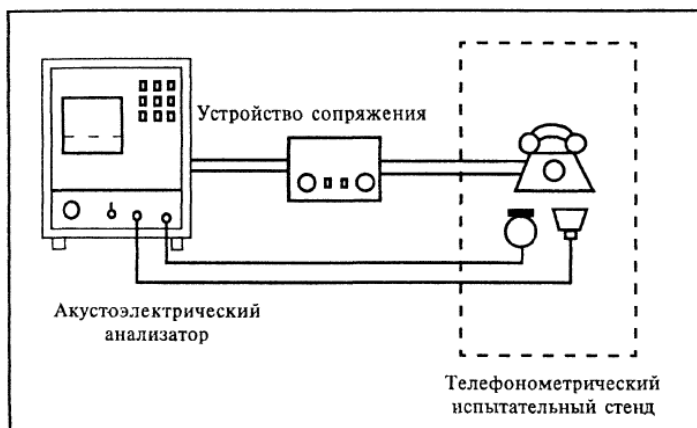


Рис. 59. Примерная схема испытаний телефонного аппарата

5.4.2. Защита от утечки за счет электромагнитного излучения [^]

Электронные и радиоэлектронные средства, особенно средства электросвязи, обладают основным электромагнитным излучением, специально вырабатываемым для передачи информации, и нежелательными излучениями, образующимися по тем или иным причинам конструкторско-технологического характера.

Нежелательные излучения подразделяются на побочные электромагнитные излучения (ПЭМИ), внеполосные и шумовые. И те и другие представляют опасность. Особенно опасны ПЭМИ. Они-то и являются источниками образования электромагнитных каналов утечки информации.

Каждое электронное устройство является источником электромагнитных полей широкого частотного спектра, характер которых определяется назначением и схемными решениями, мощностью устройства, материалами, из которых оно изготовлено, и его конструкцией.

Известно, что характер электромагнитного поля изменяется в зависимости от дальности его приема. Это расстояние делится на две зоны: ближнюю и дальнюю. Для ближней зоны расстояние r значительно меньше длины волны ($r \ll \lambda$) и поле имеет ярко выраженный магнитный характер, а для дальней — ($r \gg \lambda$) поле носит явный электромагнитный характер и распространяется в виде плоской волны, энергия которой делится поровну между электрическим и магнитным компонентами.

С учетом этого можно считать возможным образование канала утечки в ближней зоне за счет магнитной составляющей, а в дальней — за счет электромагнитного излучения.

В результате перекрестного влияния электромагнитных полей одно- или разнородного радио- и электротехнического оборудования в энергетическом помещении создается помехонесущее поле, обладающее магнитной и электрической напряженностью. Значение (величина) и фазовая направленность этой напряженности определяется числом и интенсивностью источников электромагнитных полей; размерами помещения, в котором размещается оборудование; материалами, из которых изготовлены элементы оборудования и помещения. Очевидно, чем ближе расположено оборудование относительно друг друга, чем меньше размеры помещения, тем больше напряженность электромагнитного поля.

В отношении энергетического помещения необходимо рассматривать две области распространения поля:

- внутри энергетического помещения (ближнее поле);
- за пределами помещения (дальнее поле).

Ближнее поле определяет электромагнитную обстановку в энергетическом помещении, а дальнее электромагнитное поле — распространение, дальность действия которого определяется диапазоном радиоволн.

Ближнее поле воздействует путем наведения электромагнитных полей в линиях электропитания, связи и других кабельных магистралях.

Суммарное электромагнитное поле имеет свою структуру, величину, фазовые углы напряженности, зоны максимальной интенсивности. Эти характеристики присущи как ближнему, так и дальнему полю.

В настоящее время напряженность внешних электромагнитных полей определяется с большой точностью: разработаны как аналитические, так и инструментальные методы. А вот напряженность суммарного поля, определяющая электромагнитную обстановку в энергетическом помещении, рассчитывается не достаточно строго. Нет пока четких методик расчета и методов инструментального измерения.

Таким образом, электромагнитную обстановку в помещении определяют следующие факторы:

- размеры и формы помещений;
- количество, мощность, режим работы и одновременность использования аппаратуры;
- материалы, из которых изготовлены элементы помещений и технические средства.

В качестве методов защиты и ослабления электромагнитных полей энергетического помещения используется установка электрических фильтров, применяются пассивные и активные экранирующие устройства и специальное размещение аппаратуры и оборудования.

Установка экранирующих устройств может производиться либо в непосредственной близости от источника излучения, либо на самом источнике, либо, наконец, экранируется помещение, в котором размещены источники электромагнитных сигналов.

Рациональное размещение аппаратуры и технических средств в энергетическом помещении может существенно повлиять как на результирующую напряженность электромагнитного поля внутри

помещения, так и на результирующее электромагнитное поле за его пределами. Рациональное размещение предполагает перестановку отдельных элементов оборудования помещений или отдельных групп аппаратов и технических средств с тем, чтобы новое расположение приводило к взаимокompенсации напряженности электромагнитных полей опасных сигналов в заданных зонах.

Рациональное размещение аппаратуры в отдельных случаях может оказаться определяющим.

Для реализации мероприятий по рациональному размещению аппаратуры и иного оборудования энергетических помещений с точки зрения ослабления ПЭМИН необходимо:

- иметь методику расчета электромагнитных полей группы источников опасных сигналов;
- иметь методы формализации и алгоритмы решения оптимизационных задач размещения аппаратуры.

Мероприятия по защите информации от ее утечки за счет электромагнитных излучений прежде всего включают в себя мероприятия по воспрепятствованию возможности выхода этих сигналов за пределы зоны и мероприятия по уменьшению их доступности. Развернутая структура и краткое содержание этих мероприятий приведены на рис. 60.

Следует отметить степень опасности электромагнитных излучений при реализации мероприятий по защите информации. Так как это электромагнитные волны, то особенности их распространения в пространстве по направлению и по дальности определяются диапазоном частот (длин волн) и мощностью излучения. Дальность и направленность излучения определяются физической природой распространения со-

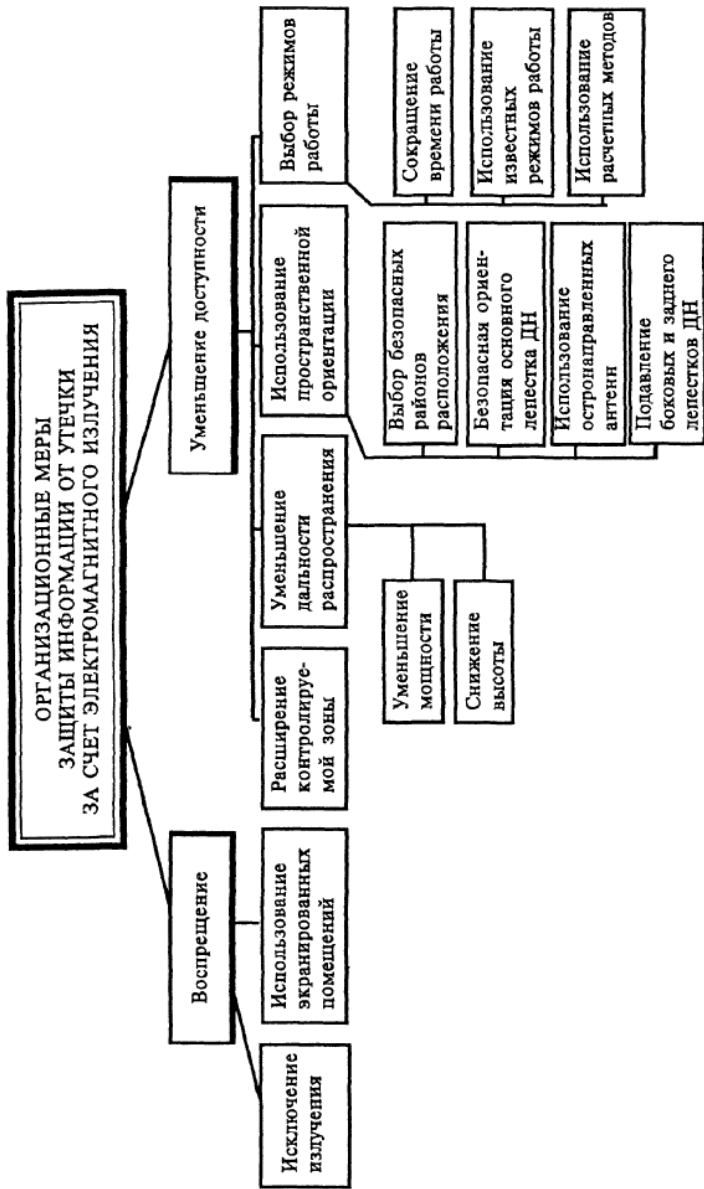


Рис 60

ответствующего вида электромагнитных волн и пространственного

расположения источника опасного сигнала и средств его приема.

Учитывая особенности распространения электромагнитных колебаний, определяющихся прежде всего мощностью излучения, особенностями распространения и величинами поглощения энергии в среде распространения, правомерно ставить вопрос об установлении их предельно допустимых интенсивностей (мощностей), потенциально возможных для приема средствами злоумышленников. Эти допустимые значения интенсивностей принято называть нормами или допустимыми значениями.

Процесс определения или выработки норм называется нормированием, которое включает прежде всего, собственно, выбор критерия нормирования, выбор и обоснование нормируемого параметра и определение его предельно допустимого значения.

Нормы могут быть международные, федеральные и отраслевые. Не исключается наличие специальных норм для конкретных изделий и предприятий.

Защита от утечки информации за счет побочных электромагнитных излучений самого различного характера предполагает:

- размещение источников и средств на максимально возможном удалении от границы охраняемой (контролируемой) зоны;
- экранирование зданий, помещений, средств кабельных коммуникаций;
- использование локальных систем, не имеющих выхода за пределы охраняемой территории (в том числе систем вторичной часофикации, радиофикации, телефонных систем внутреннего пользования, диспетчерских систем, систем энергоснабжения и т. д.);
- развязку по цепям питания и заземления, размещенных в границах охраняемой зоны;
- использование подавляющих фильтров в информационных цепях, цепях питания и заземления.

Для обнаружения и измерения основных характеристик ПЭМИ используются:

- измерительные приемники;
- селективные вольтметры;
- анализаторы спектра;
- измерители мощности и другие специальные устройства.

В качестве примера приведем характеристики отдельных

измерительных приемников и селективных вольтметров (табл. 6).

Таблица 6

| Тип | Диапазон частот | Пределы измерения мощности |
|--------|------------------|----------------------------|
| П5-34 | 8,24 – 12,05 ГГц | 3-10-12-10-4 Вт |
| П5-14 | 16,6 – 25,8 ГГц | 10-12-10-6 Вт |
| В6-9 | 20 Гц – 200 кГц | 1 мкВ – 1 В |
| В6-10 | 0,1 – 30 МГц | 1 мкВ – 1 В |
| SMV-11 | 0,01 – 30 МГц | 0,3 мкВ – 0,6 В |

Используя измерительные приемники и селективные вольтметры, измеряют мощность (или напряженность) излучения на границе контролируемой зоны, определяют соответствие ее допустимым нормам. Если нормы не выполняются, то принимают меры по ослаблению мощности излучения.

В качестве примера измерительных приемников рассмотрим программно-аппаратный комплекс «Зарница».

Он предназначен для автоматизации измерений при проведении исследований и контроля технических средств ЭВТ.

Обеспечивает: измерение параметров побочных электромагнитных излучений (ПЭМИ), обработку результатов измерений, выполнение необходимых расчетов и выпуск отчетной документации при проведении исследований и контроля технических средств ЭВТ.

Достоинства: повышение достоверности и эффективности проведения (специальных) исследований за счет автоматизации процессов измерения, выявления информативных сигналов, обработки полученных результатов в соответствии с действующими нормативно-методическими документами, выпуска отчетной документации; снижение трудозатрат на проведение исследований. При адаптации программного обеспечения комплекс может быть использован для решения задач в области электромагнитной совместимости (ЭМС) радионаблюдения и анализа электромагнитной обстановки при проведении испытаний.

Технические данные:

- измерение напряженности электромагнитного поля ПЭМИ от технических средств ЭВТ;
- работа в диапазоне частот:
 - при измерении напряженности магнитной

- составляющей поля ПЭМИ от 0,01 до 30 МГц,
- при измерении напряженности электрической составляющей поля ПЭМИ от 0,01 до 1000 МГц,
- одновременное независимое управление анализаторами спектра СК4-59 и СК4-61;
- вывод на экран монитора и принтер результатов регистрации протоколов расчетов;
- обработка результатов измерений и проведение расчетов в соответствии с действующими нормативно-методическими документами

Гарантийный срок эксплуатации — 1 год (за исключением изделий внешней поставки).

Состав системы.

- ПЭВМ типа IBM PC/AT — 1 шт.;
- Анализатор спектра СК4-59 — 1 шт.;
- Анализатор спектра СК4-61 — 1 шт.;
- Комплект входных преобразователей «АМУР-М» — 1 шт.;
- Контроллер управления АС — 2 шт.;
- Пакет прикладных программ — 1 комп.

5.4.3. Защита от утечки за счет паразитной генерации [^]

Паразитная генерация усилителей возникает из-за неконтролируемой положительной обратной связи за счет конструктивных особенностей схемы или за счет старения элементов.

Самовозбуждение может возникнуть и при отрицательной обратной связи из-за того, что на частотах, где усилитель вместе с цепью обратной связи вносит сдвиг фазы на 180° , отрицательная обратная связь превращается в положительную.

Самовозбуждение усилителей обычно происходит на высоких частотах, выходящих за пределы рабочей полосы частот (вплоть до КВ и УКВ диапазонов).

Частота самовозбуждения модулируется акустическим сигналом, поступающим на усилитель, и излучается в эфир как обычным радиопередатчиком. Дальность распространения такого сигнала определяется мощностью усилителя (т. е. передатчика) и

особенностями диапазона радиоволн.

В качестве защитных мер применяется контроль усилителей на самовозбуждение с помощью радиоприемников типа индикаторов поля, работающих в достаточно широком диапазоне частот, что обеспечивает поиск опасного сигнала.

5.4.4. Защита от утечки по цепям питания [^]

Циркулирующая в тех или иных технических средствах конфиденциальная информация может попасть в цепи и сети электрического питания и через них выйти за пределы контролируемой зоны. Например, в линию электропитания высокая частота может передаваться за счет паразитных емкостей трансформаторов блоков питания (рис. 61).

В качестве мер защиты широко используются методы развязки (разводки) цепей питания с помощью отдельных стабилизаторов, преобразователей, сетевых фильтров для отдельных средств или помещений. Возможно использование отдельных трансформаторных

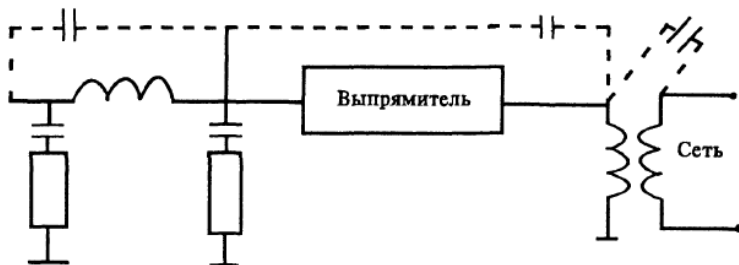


Рис. 61. Схема утечки информации по цепям питания

узел для всего энергоснабжения объекта защиты, расположенного в пределах контролируемой территории. Это более надежное решение локализации данного канала утечки.

5.4.5. Защита от утечки по цепям заземления [^]

Одним из важных условий защиты информации от утечки по цепям заземления является правильное их оборудование.

Заземление — это устройство, состоящее из заземлителей-проводников, соединяющих заземлители с электронными и

электрическими установками, приборами, машинами. Заземлители могут быть любой формы — в виде трубы, стержня, полосы, листа. Заземлители выполняют защитную функцию и предназначены для соединения с землей приборов защиты. Отношение потенциала заземлителя к стекающему с него току называется сопротивлением заземления. Величина заземления зависит от удельного сопротивления грунта и площади соприкосновения заземления с землей (рис. 62).

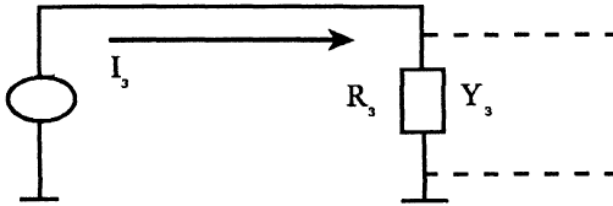


Рис. 62. Эквивалентная схема заземления

Сопротивление заземления одного контура не должно быть более 1 ома. Если заземление состоит из металлической пластины радиуса r , расположенной непосредственно у поверхности земли, то сопротивление заземления рассчитывается по формуле:

$$R_3 = \rho / 4 r,$$

где ρ — удельное сопротивление грунта, Ом/см³;
 r — радиус пластины, см;
 R_3 — сопротивление заземлителя, Ом.

Для практических расчетов удельное сопротивление грунтов можно выбрать из таблицы 7.

Таблица 7

| Грунт | r — Ом/см ³ * 10 ³ |
|---------------|--|
| Смешанный | 1 |
| Чернозем | 30 |
| Глина | 40 |
| Супесок | 30 |
| Суглинок | 10 |
| Песок влажный | 50 |
| Песок сухой | 2500 |

При устройстве заземления в качестве заземлителей чаще

всего применяются стальные трубы длиной 2 — 3 м и диаметром 25 — 50 мм и стальные полосы сечением 50— 100 мм². Заземлители следует соединять между собой шинами с помощью сварки. Сечение шин и магистралей заземления по условиям механической прочности и получения достаточной проводимости рекомендуется брать не менее 24 x 4 мм².

Магистралы заземления вне здания надо прокладывать на глубине около 1,5 м, а внутри здания — по стенам или специальным каналам таким образом, чтобы их можно было внешне осматривать на целостность и на наличие контактного подключения.

Следует отметить, что использовать в качестве заземления металлические конструкции зданий и сооружений, имеющих соединения с землей (отопление, водоснабжение), не рекомендуется.

5.4.6. Защита от утечки за счет взаимного влияния проводов и линий связи [^]

Элементы, цепи, тракты, соединительные провода и линии связи любых электронных систем и схем постоянно находятся под воздействием собственных (внутренних) и сторонних (внешних) электромагнитных полей различного происхождения, индуцирующих или наводящих в них значительные напряжения.

Такое воздействие называют электромагнитным влиянием или просто влиянием на элементы цепи. Коль скоро такое влияние образуется непредусмотренными связями, то говорят о паразитных (вредных) связях и наводках, которые также могут привести к образованию каналов утечки информации.

Основными видами паразитных связей в схемах электронных устройств являются емкостные, индуктивные, электромагнитные, электромеханические связи и связи через источники питания и заземления радиоэлектронных средств.

Паразитные емкостные связи обусловлены электрической емкостью между элементами, деталями и проводниками устройств, несущих потенциал сигнала, так как сопротивление емкости, создающей паразитную емкостную связь, падает с ростом частоты ($X_c = 1/\omega C$).

Паразитные индуктивные связи обусловлены наличием взаимоиндукции между проводниками и деталями аппаратуры, главным образом между его трансформаторами. Паразитная

индуктивная обратная связь между трансформаторами усилителя, например, между входным и выходным трансформаторами, может вызвать режим самовозбуждения в области рабочих частот и гармониках.

Паразитные электромагнитные связи обычно возникают между выводными проводниками усилительных элементов, образующими колебательную систему с распределенными параметрами и резонансной частотой определенного порядка.

Взаимные влияния в линиях связи

Рассмотрим, какое влияние друг на друга оказывают параллельно проложенные линии связи.

В теории взаимных влияний между цепями линий связи приняты следующие основные определения:

- влияющая цепь — цепь, создающая первичное влияющее электромагнитное поле;
- цепь, подверженная влиянию, — цепь, на которую воздействует влияющее электромагнитное поле;
- непосредственное влияние — сигналы, индуцируемые непосредственно электромагнитным полем влияющей цепи в цепь, подверженную влиянию.

Помимо непосредственного влияния имеют место косвенные влияния вторичными полями за счет отражений.

В зависимости от структуры влияющего электромагнитного поля и конструкции цепи, подверженной влиянию, различают систематические и случайные влияния. К систематическим влияниям относят взаимные наводки, возникающие по всей длине линии. К случайным относятся влияния, возникающие вследствие ряда случайных причин, не поддающихся точной оценке. Существуют реальные условия наводок с одного неэкранированного провода на другой, параллельный ему провод той же длины, когда оба они расположены над «землей». На рис. 63 приведены характеристики наводок.

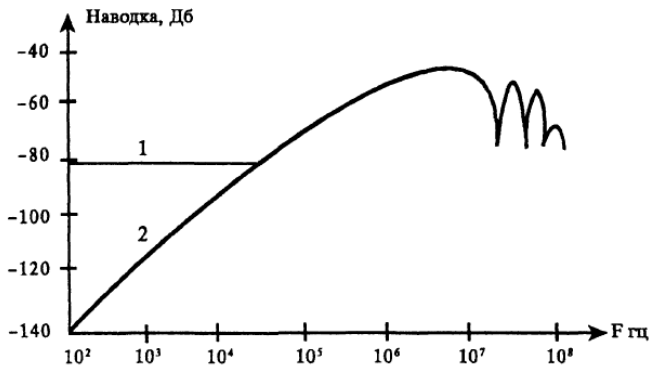


Рис. 63. Наводка на неэкранированный провод от другого неэкранированного провода при идеальной «земле» (кривая 1) и идеальной (кривая 2)

В реальных условиях имеют место наводки и от экранированных кабелей на экранированные кабели и от неэкранированных кабелей на экранированные.

На рис. 64 приведены практические результаты исследования взаимных наводок экранированных кабелей друг на друга.

Таким образом, можно заключить, что излучения и наводки от различных технических средств далеко не

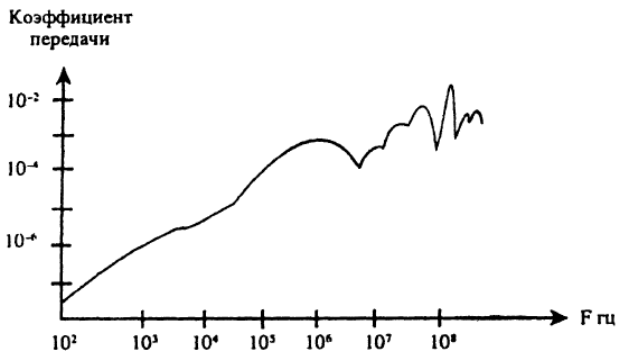


Рис. 64. Взаимные наводки экранированных кабелей безопасны. Небезопасны излучения и наводки кабельных сетей как неэкранированных, так и экранированных. Для последних

требуется хорошее состояние экрана и качественное заземление. На практике кабели не всегда полностью экранированы. Неисправные или покрытые коррозией соединители могут быть причиной значительных излучений. Используя узкополосные (полоса менее 1 кГц) приемники, можно зарегистрировать напряженности поля 0,1 мкВ на поверхности кабеля. Это позволяет обнаружить сигнал 1 мкВ на расстоянии 3 м от кабеля. Даже на расстоянии 300 м сигналы, имеющие значение 1 мВ на поверхности кабеля, могут быть обнаружены.

Различают следующие основные меры защиты цепей и трактов линий связи и проводов от взаимных влияний.

1. Применение систем передачи и типов линий связи, обеспечивающих малые значения взаимных влияний. Этот способ на практике реализуется в очень широких масштабах. Так, применение коаксиальных кабелей и волоконно-оптических линий практически полностью решает проблему защиты цепей и трактов линий связи от взаимного влияния.
2. Рациональный выбор кабелей для различных систем передачи.
3. Взаимная компенсация наводок и помех между цепями симметричных линий связи, наводимых на различных участках. Реализуется путем скрещивания цепей воздушных линий связи или симметричных кабельных линий и соответствующего подбора шагов скрутки цепей симметричного кабеля.
4. Экранирование цепей кабельных линий гибкими (чулок) или жесткими (трубы) экранами. Защита от взаимного влияния в этом случае достигается путем ослабления интенсивности влияющего электромагнитного поля в экране.

В таблице 8 приведены примерные данные взаимного влияния различных типов линий и меры их защиты.

Таблица 8

| Тип линии | Преобладающее влияние | Меры защиты |
|-----------------------|---|---|
| Воздушные линии связи | Систематическое влияние, возрастающее с увеличением частоты сигнала | Скрещивание цепей, оптимальное расположение цепей |

| | | |
|---------------------|---|--|
| Коаксиальный кабель | Систематическое влияние через третьи цепи. С повышением частоты влияние убывает вследствие поверхностного эффекта | Экранирование и ограничение диапазона рабочих частот снизу |
| Симметричный кабель | Систематическое и случайное влияния, возрастающие с частотой | Оптимизация шагов скрутки конструкции кабеля; пространственное разделение цепей, экранирование |
| Оптический кабель | Систематическое и случайное влияния от частоты сигнала практически независят | Экранирование оптических волокон, пространственное, разделение оптических волокон, защита от акустического воздействия |

5.4.7. Защита от утечки за счет высокочастотного навязывания [^]

Любое электронное устройство под воздействием высокочастотного электромагнитного поля становится как бы переизлучателем, вторичным источником излучения высокочастотных колебаний. Такой сигнал принято называть интермодуляционным излучением, а в практике специалистов бывает понятие «высоко частотное навязывание». Интермодуляционное излучение — это побочное радиоизлучение, возникающее в результате воздействия на нелинейный элемент высокочастотного электромагнитного поля и электромагнитного поля электронного устройства.

Интермодуляционное излучение в последующем может быть переизлучено на гармониках 2 и 3 порядка или наведено на провода и линии связи. Но в любом случае оно способно выйти за пределы контролируемой зоны в виде электромагнитного излучения.

В качестве источника навязываемого сигнала могут выступать:

- радиовещательные станции, находящиеся вблизи объекта защиты;
- персональные ЭВМ, электромагнитное поле которых может воздействовать на телефонные и факсимильные аппараты, с выходом опасного сигнала по проводам за пределы помещений и здания (рис. 65).

При воздействии высокочастотного навязывания на телефонный аппарат модулирующим элементом является его

микрофон. Следовательно, нужно воспрепятствовать прохождению высокочастотного тока через него. Это достигается путем подключения параллельно микрофону постоянного конденсатора емкостью порядка 0,01 — 0,05 мкФ. В этом случае высокочастотная составляющая сигнала будет проходить через конденсатор, минуя микрофон (рис. 66).

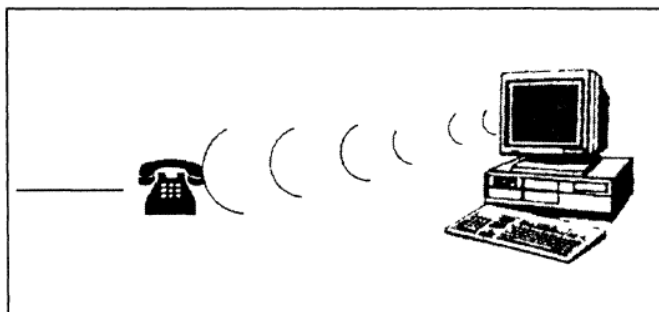


Рис. 65. Вариант высокочастотного навязывания

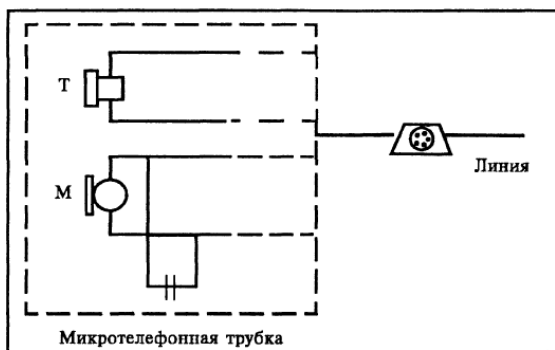


Рис. 66. Шунтирование микрофона при ВЧ-навязывании

Глубина модуляции при такой защите уменьшается более чем в 10 000 раз, что практически исключает последующую демодуляцию сигнала на приемной стороне.

Более сложной защитой является использование фильтров подавления высокочастотных сигналов на входе телефонного аппарата.

При угрозе ВЧ-навязывания лучше всего выключить телефонный аппарат на период ведения конфиденциальных переговоров.

5.4.8. Защита от утечки в волоконно-оптическим линиях и системах связи [^]

Волоконно-оптические линии связи обладают оптическими каналами утечки информации и акусто-оптическим эффектом, также образующим канал утечки акустической информации.

Причинами возникновения излучения (утечка световой информации) в разъемных соединениях волоконных световодов являются: ■ радиальная несогласованность стыкуемых волокон (рис. 67);

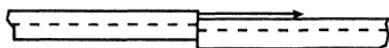


Рис. 67

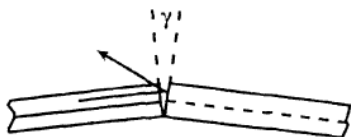


Рис. 68



Рис. 69

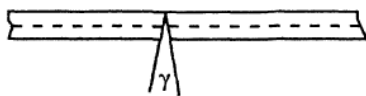


Рис. 70

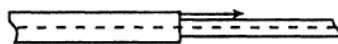


Рис. 71

- угловая несогласованность осей световодов (рис. 68);
- наличие зазора между торцами световода (рис. 69);
- наличие взаимной непараллельности поверхностей торцов волокон (рис. 70);
- разница в диаметрах сердечников стыкуемых волокон (рис. 71).

Все эти причины приводят к излучению световых сигналов в окружающее пространство.

Акусто-оптический эффект проявляется в модуляции светового сигнала за счет изменения толщины волновода под воздействием акустического давления P на волновод (рис. 72).

Защитные меры определяются физической природой возникновения и распространения света.

Для защиты необходимо оградить волновод от акустического воздействия на него.

Наружное покрытие оптического волокна в зависимости от материала покрытия может повышать или понижать чувствительность световодов к действию акустических полей. С одной стороны, акустическая

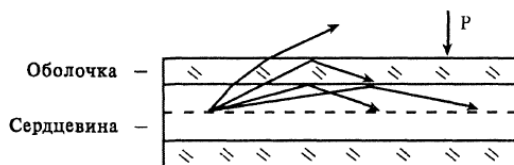


Рис. 72

чувствительность волоконного световода с полимерным покрытием может значительно превышать чувствительность оптического волокна без защитного покрытия. С другой стороны, можно значительно уменьшить чувствительность волоконно-оптического кабеля к действию акустического поля, если волокно перед его заделкой в кабель покрыть слоем вещества с высоким значением объемного модуля упругости. Это может быть достигнуто, например, нанесением непосредственно на поверхность оптического волокна слоя никеля толщиной около 13 мкм, алюминия толщиной около 95 мкм или стекла, содержащего алюминат кальция, толщиной около 70 мкм.

Применяя метод гальванического покрытия, можно получать на оптическом волокне относительно толстую и прочную пленку.

Зависимость чувствительности световодов к акустическому давлению при различных покрытиях эластомерами приведена на рис. 73.

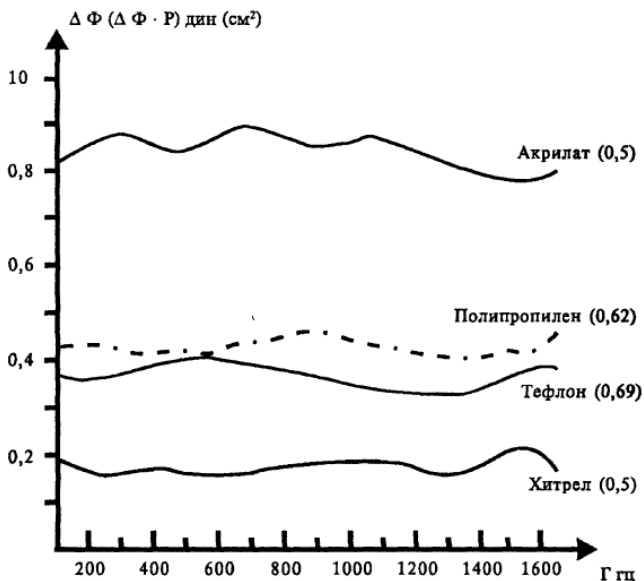


Рис. 73. Чувствительность светового волновода к оптическому давлению при различных покрытиях эластомерами. В скобках указана толщина слоя покрытия в мм

5.5. Защита информации от утечки по материально-вещественным каналам [^]

Защита информации от утечки по материально-вещественному каналу — это комплекс мероприятий, исключающих или уменьшающих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны в виде производственных или промышленных отходов.

В практике производственной и трудовой деятельности отношение к отходам, прямо скажем, бросовое. В зависимости от профиля работы предприятия отходы могут быть в виде испорченных накладных, фрагментов исполняемых документов, черновиков, бракованных заготовок деталей, панелей, кожухов и других устройств для разрабатываемых моделей новой техники или изделий.

По виду отходы могут быть твердыми, жидкими и

газообразными. И каждый из них может бесконтрольно выходить за пределы охраняемой территории. Жидкости сливаются в канализацию, газы уходят в атмосферу, твердые отходы — зачастую просто на свалку. Особенно опасны твердые отходы. Это и документы, и технология, и используемые материалы, и испорченные комплектующие. Все это совершенно достоверные, конкретные данные.

Меры защиты этого канала в особых комментариях не нуждаются.

В заключение следует отметить, что при защите информации от утечки по любому из рассмотренных каналов следует придерживаться следующего порядка действий:

1. Выявление возможных каналов утечки.
2. Обнаружение реальных каналов.
3. Оценка опасности реальных каналов.
4. Локализация опасных каналов утечки информации.
5. Систематический контроль за наличием каналов и качеством их защиты.

Выводы

1. Утечка информации — это ее бесконтрольный выход за пределы организации (территории, здания, помещения) или круга лиц, которым она была доверена. И естественно, что при первом же обнаружении утечки принимаются определенные меры по ее ликвидации.
2. Для выявления утечки информации необходим систематический контроль возможности образования каналов утечки и оценки их энергетической опасности на границах контролируемой зоны (территории, помещения).
3. Локализация каналов утечки обеспечивается организационными, организационно-техническими и техническими мерами и средствами.
4. Одним из основных направлений противодействия утечке информации по техническим каналам и обеспечения безопасности информационных ресурсов является проведение **специальных проверок (СП)** по выявлению **электронных устройств** перехвата информации и **специальных исследований (СИ)** на

побочные электромагнитные излучения и наводки **технических средств обработки** информации, аппаратуры и оборудования, в том числе и бытовых приборов.

Глава 6 ПРОТИВОДЕЙСТВИЕ НЕСАНКЦИОНИРОВАННОМУ ДОСТУПУ К ИСТОЧНИКАМ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ [^]

*Всякое действие вызывает равное ему
противодействие (Закон физики)*

Противодействие несанкционированно му доступу к конфиденциальной информации — это комплекс мероприятий, обеспечивающих исключение или ограничение неправомерного овладения охраняемыми сведениями.

Поговорки

1. В глубине всякой груди есть своя змея (К. Прутков).
2. Петух просыпается рано, но злодей — еще раньше (К. Прутков).
3. Голь на выдумки хитра.
4. С миру — по нитке, голому — рубаха.
5. Курочка по зернышку питается.
6. Кто ищет, тот всегда найдет.
7. Капля камень точит не силой, а частым падением.
8. Бойся любопытства. Любопытство — это исследование чужих дел.
9. Враг действует иногда через злых людей: через гордецов, через распутных, употребляя для этого разные обольщения.

***Несанкционированный доступ к источникам
конфиденциальной информации — это
противоправное преднамеренное овладение
конфиденциальной информацией лицом, не
имеющим права доступа к ней.***

Конкурентная борьба в условиях рыночной экономики невозможна без получения достоверной информации, а стремление

получить ее в условиях закрытого доступа порождает недобросовестную конкуренцию (потребность шпионить за конкурентом). Экономическая сущность недобросовестной конкуренции ясна — не тратить средства на проведение разработок и получение новой продукции (на это требуются, как правило, огромные средства), а, потратив незначительную часть этой суммы на противозаконные действия, получить требуемую информацию у конкурента и таким образом получить большую прибыль. Преследуются и другие цели: уничтожить конкурента, сорвать ему выгодные сделки, понизить престиж фирмы и т. д.

Чтобы добыть коммерческие секреты, злоумышленники имеют необходимые кадры, технические средства и отработанные способы и приемы действий. Какие же способы несанкционированного доступа к источникам конфиденциальной информации используются злоумышленниками?

6.1. Способы несанкционированного доступа [^]

В отечественной и зарубежной литературе имеет место различное толкование как понятия способа несанкционированного доступа, так и его содержание. Под способом вообще понимается порядок и приемы действий, приводящие к достижению какой-либо цели. Энциклопедическое понимание способа производства — исторически обусловленная форма производства материальных благ. Известно также определение способов военных действий, как порядок и приемы применения сил и средств для решения задач в операции (бою). С учетом рассмотренного, можно так определить способ несанкционированного доступа: это совокупность приемов, позволяющих злоумышленнику получить охраняемые сведения конфиденциального характера.

В работе «Предприниматель и безопасность» автор приводит перечень способов несанкционированного доступа к источникам конфиденциальной информации и дает краткое изложение их содержания. По нашему мнению, способами несанкционированного доступа являются:

1. Инициативное сотрудничество.
2. Склонение к сотрудничеству.
3. Выведывание, выпытывание.
4. Подслушивание.
5. Наблюдение.
6. Хищение.

7. Копирование.
8. Подделка (модификация).
9. Уничтожение.
10. Незаконное подключение.
11. Перехват.
12. Негласное ознакомление.
13. Фотографирование.
14. Сбор и аналитическая обработка информации.

Инициативное сотрудничество проявляется в определенных действиях лиц, чем-то неудовлетворенных или остро нуждающихся в средствах к существованию, из числа работающих на предприятии или просто алчных и жадных, готовых ради наживы на любые противоправные действия. Известно достаточно примеров инициативного сотрудничества по политическим, моральным или финансовым соображениям, да и просто по различным причинам и побуждениям. Финансовые затруднения, политическое или научное инакомыслие, недовольство продвижением по службе, обиды от начальства и властей, недовольство своим статусом и многое другое толкают обладателей конфиденциальной информации на сотрудничество с преступными группировками и иностранными разведками. Наличие такого человека в сфере производства и управления предприятия позволяет злоумышленникам получать необходимые сведения о деятельности фирмы и очень для них выгодно, т. к. осведомитель экономит время и расходы на внедрение своего агента, представляет свежую и достоверную информацию, которую обычным путем было бы сложно получить.

Склонение к сотрудничеству — это, как правило, насильственное действие со стороны злоумышленников. Склонение или вербовка может осуществляться путем подкупа, запугивания, шантажа. Склонение к сотрудничеству реализуется в виде реальных угроз, преследования и других действий, выражающихся в преследовании, оскорблении, надругательстве и т. д. Шантаж с целью получения средств к существованию, льгот, политических выгод в борьбе за власть практикуется с легкостью и завидным постоянством. Некоторые конкуренты не гнушаются и рэкетом. По интенсивности насилия это один из наиболее агрессивных видов деятельности, где за внешне мирными визитами и переговорами кроется готовность действовать намеренно жестоко с целью устрашения. Весьма близко к склонению лежит и переманивание специалистов фирмы конкурента на свою фирму с целью последу-

ющего обладания его знаниями.

Выведывание, выпытывание — это стремление под видом наивных вопросов получить определенные сведения. Выпытывать информацию можно и ложными трудоустройствами, и созданием ложных фирм, и другими действиями.

Подслушивание — способ ведения разведки и промышленного шпионажа, применяемый агентами, наблюдателями, информаторами, специальными постами подслушивания. В интересах подслушивания злоумышленники идут на самые различные ухищрения, используют для этого специальных людей, сотрудников, современную технику, различные приемы ее применения. Подслушивание может осуществляться непосредственным восприятием акустических колебаний лицом при прямом восприятии речевой информации либо с помощью технических средств.

Наблюдение — способ ведения разведки о состоянии и деятельности противника. Ведется визуально и с помощью оптических приборов. Процесс наблюдения довольно сложен, так как требует значительных затрат сил и средств. Поэтому наблюдение, как правило, ведется целенаправленно, в определенное время и в нужном месте специально подготовленными людьми, ведется скрытно. К техническим средствам относятся оптические приборы (бинокли, трубы, перископы), телевизионные системы (для обычной освещенности и низкоуровневые), приборы наблюдения ночью и при ограниченной видимости.

Хищение — умышленное противоправное завладение чужим имуществом, средствами, документами, материалами, информацией. Похищают все, что плохо лежит, включая документы, продукцию, диски, ключи, коды, пароли и шифры.

Копирование. В практике криминальных действий копируют документы, содержащие интересующие злоумышленника сведения; информацию, обрабатываемую в АСОД (автоматизированные системы обработки данных); продукцию.

Подделка (модификация, фальсификация) в условиях беззащитной конкуренции приобрела большие масштабы. Подделывают доверительные документы, позволяющие получить определенную информацию, письма, счета, бухгалтерскую и финансовую документацию, ключи, пропуска, пароли и т. д.

Уничтожение. В части информации особую опасность представляет ее уничтожение в АСОД, в которой накапливаются на

технических носителях огромные объемы сведений различного характера, причем многие из них весьма трудно изготовить в виде немашинных аналогов. Уничтожаются и люди, и документы, и средства обработки информации, и продукция.

Незаконное подключение. Под незаконным подключением будем понимать контактное или бесконтактное подключение к различным линиям и проводам с целью несанкционированного доступа к информации. Незаконное подключение как способ тайного получения информации известен давно. Подключение возможно как к проводным линиям телефонной и телеграфной связи, так и к линиям связи иного информационного назначения: линиям передачи данных, соединительным линиям периферийных устройств больших и малых ЭВМ, линиям диспетчерской связи, конференц-связи, питания, заземления и другими.

Перехват. В практике радиоэлектронной разведки под перехватом понимают получение разведывательной информации за счет приема сигналов электромагнитной энергии пассивными средствами приема, расположенными, как правило, на достаточном расстоянии от источника конфиденциальной информации. Перехвату подвержены переговоры любых систем радиосвязи, переговоры, ведущиеся с подвижных средств телефонной связи (радиотелефон), переговоры внутри помещения посредством бесшнуровых систем учрежденческой связи и другие.

Негласное ознакомление — способ получения информации, к которой субъект не допущен, но при определенных условиях он может получить возможность кое-что узнать (открытый документ на столе во время беседы с посетителем, наблюдение экрана ПЭВМ со значительного расстояния в момент работы с закрытой информацией и т. д.). К негласному ознакомлению относится и перлюстрация почтовых отправлений, учрежденческой и личной переписки.

Фотографирование — способ получения видимого изображения объектов криминальных интересов на фотоматериале. Особенность способа — документальность, позволяющая при дешифровании фотоснимков по элементам и демаскирующим признакам получить весьма ценные, детальные сведения об объекте наблюдения.

Сбор и аналитическая обработка являются завершающим этапом изучения и обобщения добытой информации с целью получения достоверных и объемлющих сведений по интересующему злоумышленника аспекту деятельности объекта

его интересов. Полный объем сведений о деятельности конкурента не может быть получен каким-нибудь одним способом. Чем большими информационными возможностями обладает злоумышленник, тем больших успехов он может добиться в конкурентной борьбе. На успех может рассчитывать тот, кто быстрее и полнее соберет необходимую информацию, переработает ее и примет правильное решение.

На наш взгляд, такой перечень является независимым и непересекаемым на выбранном уровне абстракции, что позволяет рассмотреть определенное множество способов с увязкой со множеством источников конфиденциальной информации. Даже беглый обзор позволяет заключить, что к определенным источникам применимы и определенные способы. Не вдаваясь в сущность каждого способа несанкциони-

ОБЩЕННАЯ МОДЕЛЬ
способов несанкционированного доступа к источникам конфиденциальной информации

| №ФФ п/п | Источники | Способы | | | | | | | | | | | | | | |
|------------|------------------------------|--------------------------------|-------------------------------|-------------|---------------|------------|---------|-------------|---------------------------|------------------------------------|---------------------------|----------|--------------------------|------------------|-----------------------------------|----------------------------------|
| | | инициативное сотрудничество | склопение к сотрудничеству | выпытывание | подслушивание | наблюдение | хищение | копирование | подделка (модификация) | уничтожение (порча, разрушение) | незаконное подключение | перехват | неласное ознакомление | фотографирование | сбор и аналитическая обработка | общее количество по источнику |
| 1 | Люди | ⊕ | ⊕ | ⊕ | ⊕ | ⊕ | ⊕ | | | | | | ⊕ | ⊕ | | 10 |
| 2 | Документы | | | | | ⊕ | ⊕ | ⊕ | ⊕ | | | ⊕ | ⊕ | ⊕ | ⊕ | 9 |
| 3 | Публикации | | | | | | | | | | | ⊕ | | | ⊕ | 3 |
| 4 | Технические носители | | | | | | | | | | ⊕ | | | | ⊕ | 5 |
| 5 | Технические средства ОПД | | | | ⊕ | | | | | | | ⊕ | | | | 4 |
| 6 | Технические средства АСОД | | | | ⊕ | ⊕ | ⊕ | ⊕ | ⊕ | ⊕ | ⊕ | ⊕ | ⊕ | ⊕ | | 10 |
| 7 | Продукция | | | | | ⊕ | ⊕ | ⊕ | | | | | ⊕ | ⊕ | | 7 |
| 8 | Отходы | | | | | | | | | | ⊕ | | | | ⊕ | 2 |
| | ИТОГО | 1 | 1 | 1 | 3 | 4 | 6 | 4 | 6 | 4 | 4 | 3 | 5 | 4 | 4 | 50 |

Рис 74

рованного доступа (СНСД), на общем уровне видно, что они могут

быть сгруппированы с учетом физической природы реализации в определенные группы или направления в части решения задач противодействия им (рис. 74).

В общем плане мероприятия по противодействию несанкционированному доступу к источникам конфиденциальной информации с помощью технических средств можно свести к следующим основным направлениям:

- защита от наблюдения и фотографирования;
- защита от подслушивания;
- защита от незаконного подключения;
- защита от перехвата.

6.2. Технические средства несанкционированного доступа к информации [^]

Акустический контроль. К системам акустического контроля относится широкая номенклатура различных радиомикрофонов, назначением которых является съём информации и передача ее по радиоканалу.

Радиомикрофоны — это специальные устройства съема информации, которые по своему исполнению бывают:

- простейшие — непрерывно излучающие;
- с включением на передачу при появлении в контролируемом помещении разговоров или шумов;
- дистанционно управляемые — включающиеся и выключающиеся дистанционно на время, необходимое для контроля помещения. Специальные устройства съема информации и передачи ее по радиоканалу можно классифицировать по следующим признакам:
 - диапазону используемых частот (от 27 МГц до 1,5 ГГц и выше);
 - продолжительности работы (от 5 часов до 1 года);
 - радиусу действия (от 15 м до 10 км).;
 - виду модуляции (АМ, ЧМ, узкополосная ЧМ, однополосная АМ, широкополосная шумоподобная).

Следует отметить, что в последнее время появились специальные устройства съема информации, использующие для передачи акустической информации так называемые «нетрадиционные каналы». К этим каналам можно отнести следующие:

Устройства съема информации, ведущие передачу в

инфракрасном диапазоне (ИК передатчики). Характеризуются такие изделия крайней сложностью их обнаружения. Срок непрерывной работы — 1—3 суток. Используют эти устройства, как правило, для увеличения дальности передачи информации и размещаются у окон, вентиляционных отверстий и т. п., что может облегчить задачу их поиска. Для приема информации применяют специальный приемник ИК диапазона, который обеспечивает надежную связь на расстоянии 10—15 м.

Устройства съема информации, использующие в качестве канала передачи данных силовую электрическую сеть 127/220/380 В. Такие устройства встраиваются в электрические розетки, удлинители, тройники, бытовую аппаратуру и другие места, где проходит или подключается сеть. К основным достоинствам таких устройств можно отнести неограниченное время работы. Прием информации от таких устройств осуществляется специальными приемниками, подключаемыми к силовой сети, в радиусе до 300 м.

Устройства съема информации с ее закрытием, использующие шифровку или преобразование частоты с различными видами модуляции. Попытка прослушать такое устройство даже очень хорошим сканирующим приемником ни к чему не приведет — будет слышен лишь шум, указывающий только на наличие устройства съема информации.

Устройства съема информации на основе лазерного микрофона, который позволяет на расстоянии до 300 м регистрировать колебания оконных стекол и преобразовывать их в звуковой сигнал.

Устройства съема информации, использующие «нетрадиционные каналы» передачи, чрезвычайно дороги и сложны в эксплуатации, поэтому использование их частными лицами маловероятно.

В тех случаях, когда нельзя установить устройства съема информации непосредственно на объекте, применяют стетоскопные микрофоны, которые позволяют прослушивать переговоры через твердую преграду (стену, стекло, корпус автомобиля и т. п.), причем, чем тверже и однороднее преграда, тем лучше они работают. Стетоскоп представляет собой вибродатчик с усилителем и головными телефонами (или устройством автоматической записи звука на магнитную ленту). С помощью стетоскопного микрофона можно осуществлять прослушивание разговоров через стену толщиной 1 м и более. Основным преимуществом такой системы является трудность ее обнаружения, т. к. стетоскопный микрофон

можно устанавливать в соседнем помещении. Устройства съема информации устанавливаются с согласия хозяина помещения или без его в специально подготовленные места с последующей их маскировкой либо встраиваются в предметы быта, интерьера или свободные полости помещения.

Контроль и прослушивание тещ о иных каналов связи

В последнее время одним из основных способов несанкционированного доступа к информации частного и коммерческого характера стало прослушивание телефонных переговоров. Для прослушивания телефонных переговоров используются следующие способы подключения:

- параллельное подключение к телефонной линии. В этом случае телефонные радиоретрансляторы труднее обнаруживаются, но требуют внешнего источника питания;
- последовательное включение телефонных радиоретрансляторов в разрыв провода телефонной линии. В этом случае питание телефонного радиоретранслятора осуществляется от телефонной линии, и в эфир он выходит (т. е. начинает передачу) с момента подъема телефонной трубки абонентом.

Подключение телефонного радиоретранслятора может осуществляться как непосредственно к телефонному аппарату, так и на любом участке линии от телефона абонента до АТС. В настоящее время существуют телефонные радиоретрансляторы, позволяющие прослушивать помещение через микрофон лежащей трубки. Для этого на один провод телефонной линии подаются сигнал от генератора высокочастотных колебаний, а к другому — подключают амплитудный детектор с усилителем. В этом случае высокочастотные колебания проходят через микрофон или элементы телефонного аппарата, обладающие «микрофонным эффектом», и модулируются акустическими сигналами прослушиваемого помещения. Промодулированный высокочастотный сигнал демодулируется амплитудным детектором и после усиления готов для прослушивания или записи. Дальность действия такой системы из-за затухания ВЧ сигнала в двухпроводной линии не превышает нескольких десятков метров. Существуют системы прослушивания телефонных разговоров, не требующие непосредственного электронного соединения с телефонной линией. Эти системы используют индуктивный способ

(при помощи катушек) съема информации. Они достаточно громоздки, поскольку содержат несколько каскадов усиления слабого НЧ сигнала и обязательный внешний источник питания. Поэтому такие системы не нашли широкого практического применения. Для приема информации от телефонных радиотрансляторов используются такие же приемники, как в акустических устройствах съема информации по радиоканалу. В настоящее время появились системы перехвата фак-совой и модемной связи, которые при использовании персонального компьютера со специальным программным обеспечением позволяют получить расшифровку информации. Однако такие системы очень дорогие и пока не нашли широкого применения в нашей стране. Способы, которыми может вестись прослушивание телефонных линий, и какая при этом используется аппаратура. Кратко рассмотрим эти способы.

Непосредственное подключение к телефонии и линии

Непосредственное подключение к телефонной линии — наиболее простой и надежный способ получения информации. В простейшем случае применяется трубка ремонтника-телефониста, подключаемая к линии в распределительной коробке, где производится разводка кабелей. Чаще всего, это почерк «специалистов» нижнего звена уголовного мира (верхнее звено оснащено аппаратурой не хуже государственных секретных служб). Необходимо помнить, что АТС переключает линию на разговор при шунтировании ее сопротивлением около 1 кОм. Применение аппаратуры подслушивания с низкоомным входным сопротивлением можно достаточно быстро обнаружить. Если вы услышите щелчки в линии или перепады громкости — есть вероятность того, что вас пытаются прослушать не совсем профессиональным способом.

Подкуп персонала АТС

Подкуп обслуживающего персонала на АТС — весьма распространенный способ раскрытия ваших секретов. Особенно это касается небольших городов, где до сих пор используются старые декадно-шаговые АТС. Скорее всего, таким способом могут воспользоваться преступные группы либо конкурирующие фирмы.

Прслушивание через электро магнитный звонок

Телефонные аппараты, где в качестве вызывного устройства используется электромагнитный звонок, пока еще широко распространены в нашей стране. Звонок обладает свойством дуальности, то есть, если на электромагнитный звонок действуют звуковые волны, он начнет вырабатывать соответствующим образом модулированный ток. Амплитуда его достаточна для дальнейшей обработки. Эксперименты показали, что амплитуда ЭДС, наводимая в линии, для некоторых типов телефонных аппаратов может достигать нескольких милливольт. Корпус аппарата является до полнительным резонирующим устройством

Прслушивание через микрофон тец о оно го аппарата

Этот способ не является синонимом непосредственного подключения к линии. Он гораздо сложнее. Микрофон является частью электронной схемы телефонного аппарата: он либо соединен с линией (через отдельные элементы схемы) при разговоре, либо отключен от нее, когда телефонный аппарат находится в готовности к приему вызова (трубка находится на аппарате). На первый взгляд, когда трубка лежит на аппарате, нет никакой возможности использовать микрофон в качестве источника съема информации. Но это только на первый взгляд. Для защиты телефонного аппарата от снятия информации таким способом достаточно параллельно микрофону подключить конденсатор емкостью 0,01 — 0,05 мкФ. При этом последний будет шунтировать микрофон по высокой частоте и глубина модуляции ВЧ колебаний уменьшится более чем в 10 000 раз, что делает дальнейшую демодуляцию сигнала практически невозможной.

Перехват компьютерной информации, несанкционированное внедрение в базы данных

Стандартность архитектурных принципов по строения оборудования и программного обеспечения определяет сравнительно легкий доступ профессионала к информации, находящейся в персональном компьютере (ПК). Ограничение доступа к ПК путем введения кодов не обеспечивает полной защиты информации. Включить компьютер и снять код доступа к системе не вызывает особых затруднений — достаточно отключить

аккумулятор на материнской плате. На некоторых моделях материнских плат для этого предусмотрен специальный переключатель. Также у каждого изготовителя программы BIOS (AMI, AWARD и др.) есть коды, имеющие приоритет перед любыми пользовательскими, набрав которые можно получить доступ к системе. В крайнем случае, можно украсть системный блок компьютера или извлечь из него жесткий диск и уже в спокойной обстановке получить доступ к необходимой информации. Другое дело, когда попасть в помещение, где установлен компьютер, не удастся. В этом случае используют дистанционные способы съема информации. Естественно, они эффективны только тогда, когда компьютер включен. Существует два способа дистанционного считывания информации: первый способ основан на приеме ВЧ наводок в силовую сеть, а второй — на приеме побочных электромагнитных излучений соединительных цепей ПК. Распространение побочных электромагнитных излучений за пределы контролируемой территории создает предпосылки для утечки информации, так как возможен ее перехват с помощью специальных технических средств контроля. В персональном компьютере основными источниками электромагнитных излучений являются монитор и соединительные цепи (устройства ввода и вывода информации). Утечке информации в ПК способствует применение коротких видеоимпульсов прямоугольной формы и высокочастотных коммутирующих сигналов. Исследования показывают, что излучение видеосигнала монитора является достаточно мощным, широкополосным и охватывает диапазон метровых и дециметровых волн. Причиной мощного излучения является наложение радиосигнала на импульсы развертки изображения, вырабатываемые строчным трансформатором. При кажущейся сложности проблемы, аппаратура для этого вида коммерческой разведки достаточно проста и изготавливается на базе обычного малогабаритного телевизора. Такие устройства позволяют на удалении 50 м получать устойчивую картинку — копию изображения, отображаемого в настоящий момент на экране монитора вашего ПК. Для уменьшения уровня побочных электромагнитных излучений применяют специальные средства защиты информации: экранирование помещений, фильтрацию источников питания, дополнительное заземление, электромагнитное заземление, а также средства ослабления уровней нежелательных электромагнитных излучений и наводок при помощи различных

резистивных и поглощающих согласованных нагрузок. В последнее время все чаще говорят о несанкционированном внедрении в базы данных. Этот вид пиратства очень быстро развивается вследствие бурного развития компьютеризации при обработке информации в коммерческих кругах с выходом информационных сетей в телефонную сеть общего пользования. Компьютерные взломщики, «хакеры», не ограничиваются вопросами бесплатного получения коммерческой информации — достаточно случаев вскрытия и перевода денежных счетов из одного банка в другой через информационную сеть общего пользования.

Скрытая фото- и видеосъемка при помощи специальной оптики

Не нужно обращаться к истории разведки, чтобы сделать вывод о том, что визуальное наблюдение является самым древним и очень эффективным методом сбора информации. В настоящее время для сбора информации могут использоваться миниатюрные скрытые и специальные (камуфлированные под обычные предметы) фото- и видеокамеры:

- миниатюрные (скрытые) встраиваются в бытовую технику и передают видеoinформацию по кабелю или по ВЧ каналу при помощи телевизионного передатчика;
- специальные, т. е. замаскированные под бытовые предметы, например, пачку сигарет, кейс, книгу, наручные часы и т. п.

Аппаратура для скрытой фото- и видеосъемки, как правило, оборудуется специальными объективами и насадками:

- миниатюрными объективами, предназначенными для съемки через отверстия небольшого диаметра (до 5 мм);
- телескопическими объективами, позволяющими вести съемку с дальних расстояний. Такие объективы обладают высокой кратностью увеличения (до 1,5 тыс. крат);
- комифляжными объективами, используемыми для скрытой съемки из различных бытовых предметов, например, из кейсов;
- объективами, совмещенными с приборами ночного видения (с инфракрасной подсветкой) и предназначенными для проведения съемки в темное время суток.

В качестве примера оборудования для скрытого наблюдения рассмотрим миниатюрную телевизионную камеру JT-24Is, которая

позволяет сделать это наблюдение абсолютно незаметным, информативным и безопасным. Использование телекамеры JT-24 Is наиболее эффективно в системах охраны, системах телевизионного наблюдения, системах скрытого аудиовидеопотокола и т. д. Сверхминиатюрный зрачок объектива позволяет вести наблюдение через отверстие диаметром 0,3—1,2 мм при угле поля зрения 110° , а высокая чувствительность (0,04 лк) — видеть в темноте лучше, чем человеческий глаз. Малые размеры телекамеры (39x39x20 мм) позволяют установить ее в любые элементы интерьера: часы, книгу, картину, входную дверь, стену и т. п. Телекамера может быть оснащена другими объективами с иным полем зрения. Перечень техники фото- и видеосъемки можно было бы продлить, но вероятность ее использования частными лицами очень мала из-за сложности в эксплуатации и большой стоимости.

6.3. Защита от наблюдения и фотографирования [^]

Наблюдение — способ ведения разведки с целью получения информации об объекте визуальным путем или путем применения оптических средств.

Ведется наблюдение за людьми, их перемещением пешком и на транспорте, за встречами, другими действиями; а также помещениями. В дневное время процесс наблюдения облегчается за счет высокого уровня освещенности и полного использования функциональных возможностей зрения. В ночное время эти возможности ограничены настолько, что человек даже на открытой местности способен наблюдать только крупногабаритные объекты.

Наблюдение — это постоянное, периодическое или выборочное активное и целенаправленное исследование предметов, документов, явлений, действий и людей в естественных условиях жизни, быта, производства с последующим обобщением и анализом данных наблюдения.

Наблюдение различается по виду, длительности, интенсивности и целям. Наблюдение может вестись на расстоянии прямой видимости и на больших расстояниях с помощью специальных оптических систем и систем телевидения.

Целенаправленное изучение объекта путем наблюдения позволяет например, обнаружить или установить подготовку определенных организационных или производственно-коммерческих мероприятий.

В целях документирования фактов наблюдения и

последующего анализа наблюдение зачастую сопровождается фотографированием или видеозаписью деятельности объекта наблюдения. Известно, что фотографирование (видеозапись) требует соблюдения определенных условий. Эти условия представляются в виде модели фотографического контакта (рис. 75).

Защита от наблюдения и фотографирования предполагает:

- выбор оптимального расположения средств документирования, размножения и отображения (экраны ПЭВМ, экраны общего пользования и др.) информации с целью исключения прямого или дистанционного наблюдения (фотографирования);
- использование светонепроницаемых стекол, занавесок, драпировок, пленок и других защитных материалов (решетки, ставни и пр.);
- выбор помещений, обращенных окнами в безопасные зоны (направления);
- использование средств гашения экранов ЭВМ и табло коллективного пользования после определенного времени работы (работа по режиму времени).

Защита от наблюдения и фотографирования на местности предполагает применение мер маскирования, скрытия объектов в рельефе местности, лесных массивах и, естественно, организацию режима охраны на удалении, обеспечивающей скрытность деятельности.

В более сложных условиях можно применять средства активного маскирования: маскирующие дымы, аэрозоли и другие средства.

6.4. Защита от подслушивания [^]

Подслушивание — способ ведения разведки и промышленного шпионажа, применяемый агентами, наблюдателями, специальными постами подслушивания, всеми разведывательными подразделениями. Ведется также подслушивание переговоров и сообщений, передаваемых по техническим средствам связи.

Известно, что подслушивание может быть непосредственное, когда акустические колебания говорящего прямо или через конструкции зданий и помещений достигают подслушивающего. Однако широко распро-

ЧАСТНАЯ МОДЕЛЬ
фотографического контакта

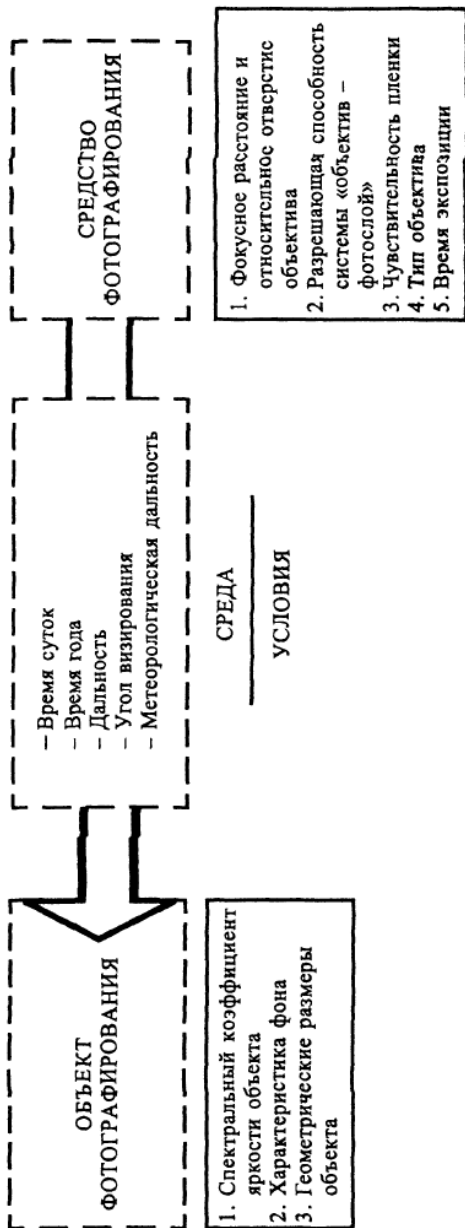


Рис. 75

странено подслушивание переговоров с использованием различных технических средств: микрофонов, радиозакладок, лазеров, высокочастотных колебаний (рис. 76).



Рис. 76

6.4.1. Противодействие подслушиванию посредством микрофонных систем [^]

Микрофон является первым звеном в системе подслушивания с помощью технических средств как микрофонных,

так и радиозакладных. Каждый микрофон обладает двумя основными параметрами:

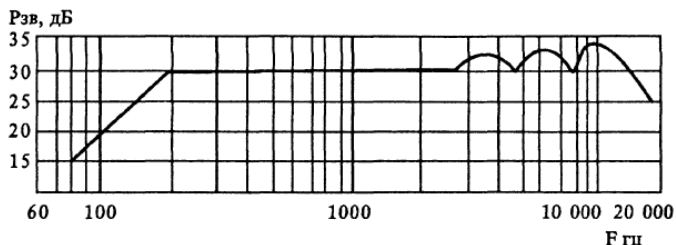


Рис. 77. Частотная характеристика микрофона MD-16N

- чувствительностью. Чувствительность — это отношение напряжения на выходе микрофона к воздействию на него звуковому давлению, выраженному в милливольт на паскаль (мВ/Па);
- частотной характеристикой. Частотная характеристика — это зависимость чувствительности от частоты звукового давления. На рис. 77 приведена частотная характеристика динамического микрофона MD-16N, а в таблице 9 приведены основные обобщенные характеристики некоторых групп микрофонов.

Таблица 9

Некоторые характеристики микрофонов

| Класс | Параметры | |
|-------------------------|--------------------------|---------------|
| | Чувствительность (мВ/Па) | Диапазон (Гц) |
| Бытовые микрофоны | 2 | 80 – 10000 |
| Универсальные микрофоны | 1,5 | 50 – 12500 |
| Студийные микрофоны | 1,5 | 40 – 20000 |

Известно, что звуковое давление по степени его восприятия человеком можно классифицировать на слышимый звук, лежащий в полосе 16 — 20 000 Гц, инфразвук — ниже 16 Гц, и ультразвук, диапазон частот которого находится выше 20 000 Гц.

В качестве меры противодействия избирается акустическое воздействие на микрофон частотами ульт-

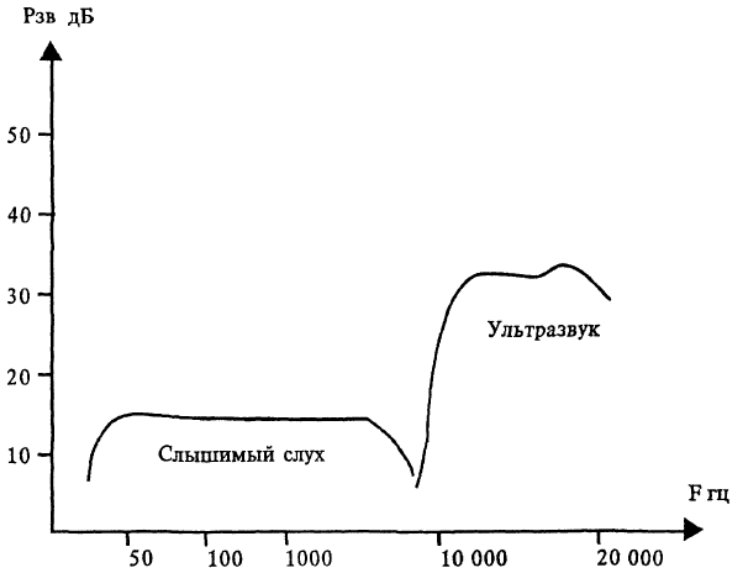


Рис. 78

развучкового диапазона. Такое воздействие не мешает ведению переговоров, но полностью подавляет воздействие речевого сигнала большим по величине давлением ультразвука (рис. 78).

В разделе 5.3.2 рассмотрен пример генератора ультразвуковых колебаний.

Воспринимаемый микрофоном звук преобразуется в электрические колебания, которые тем или иным способом необходимо передать соответствующим устройствам их приема и обработки.

Каким бы путем подслушивающий микрофон ни был доставлен (установлен) в помещение — принесен и закамouflирован либо принесен злоумышленником на себе (на теле) или в каких-либо предметах (кейс, сумка и др.), — его сигналы могут быть либо записаны на магнитофон (микрофон соединен проводом с системой записи), либо переданы по проводам или эфиру. Способы коммуникации сигналов от закладных микрофонов приведены на рис. 79.

Одним из вариантов дистанционного управляемого микрофона является так называемое «телефонное ухо» - в этом устройстве микрофон и схема управления микрофоном и телефонным аппаратом устанавли-

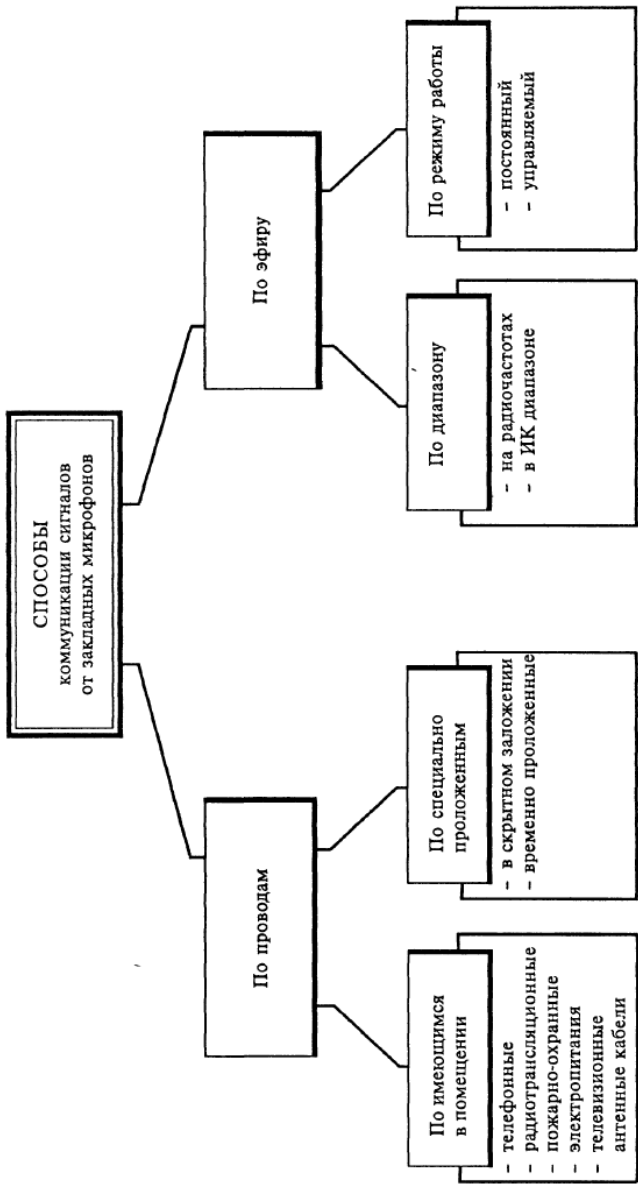


Рис. 79

вается злоумышленником в разъемную телефонную розетку. Такое устройство предназначено для подслушивания разговоров в офисе,

квартире и в других помещениях, с любого другого телефона города и даже из других городов и стран. Для включения в работу подслушивающего микрофона необходимо набрать номер телефонного аппарата, на который это устройство поставлено. После набора номера устройство работает так:

- первый звонок перехватывает и переходит в активный режим;
- при втором звонке через 10—15 сек. дает ложные гудки «занято» в течение 40 сек., после чего гудки прекращаются и включается микрофон, расположенный в розетке, и начинается подслушивание.

В случае, если абонент поднимет трубку, чтобы позвонить кому-нибудь, прослушивание прекращается, не выдавая себя ничем. При обычном звонке оно также себя не обнаруживает (рис. 80).

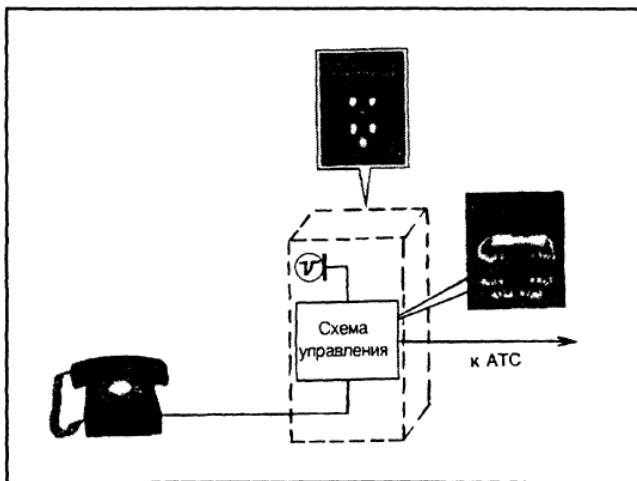


Рис. 80. Общая схема «телефонного уха»

Основные ТТХ:

- Акустическая чувствительность микрофона — до 10 м.
- Электропитание — от телефонной линии.
- Длительность непрерывной работы — неограниченная.
- Дальность действия — неограниченная.
- Включение модуля осуществляется дистанционно с помощью обычного телефонного аппарата путем

набора спецномера.

Для подслушивания, а вернее, тайной записи переговоров, используются магнитофоны (диктофоны), также имеющие встроенный и удаленный микрофон. В этом случае необходимо вначале определить наличие таких устройств у посетителя, а затем уже противодействовать его использованию.

Для обнаружения магнитофонов используются портативные и стационарные средства и системы. Обнаружение осуществляется по электромагнитному полю электрического двигателя, обеспечивающего продвижение записывающего носителя (магнитная лента, магнитная проволока и др.). Так, на нашем рынке имеется портативный обнаружитель TRD-800 (США), обеспечивающий обнаружение магнитного поля на дальность до 15 см, стационарный обнаружитель PTRD-012 и PTRD-014 (США), обеспечивающий обнаружение магнитофонов (по проспекту) до 2 — 3 метров.

Устройство PTRD-014 предназначено для охраны помещений от несанкционированного использования портативных звукозаписывающих устройств (магнитофонов, диктофонов и пр.).

Для данной модели информативным сигналом является электромагнитное поле, создаваемое работающим мотором диктофона. Это является принципиальным отличием от существующих на рынке спецтехники систем аналогичного назначения, реагирующим на генератор тока стирания и подмагничивания (ГСП), отсутствующий у подавляющего большинства используемых в данное время диктофонов.

Оригинальные технические решения, используемые в устройстве, позволили решить задачу обнаружения средств звукозаписи на фоне внешних помех, в 10 000 раз превышающих уровень полезного сигнала.

Устройство в максимальной степени адаптировано к работе в условиях сложной помеховой электромагнитной обстановки.

Технические характеристики:

- дальность обнаружения — 0,5—1,5 м;
- питание — 220 В / 50 Гц;
- габариты датчика — 240x180x22 мм;
- габариты основного блока — 180x180x22 мм;
- длина соединительного кабеля — до 3 м.

Известна и система обнаружения диктофонов типа RM-200. Система устанавливается в служебном помещении, как правило, ориентированном на ведение переговоров. Под каждым жестко

закрепленным к полу креслом (вращающимся) закрепляется решетка магнитных датчиков, подключенных к устройству обработки сигналов и индикации, определяющему, на каком месте за столом выявлен работающий диктофон (рис. 81).

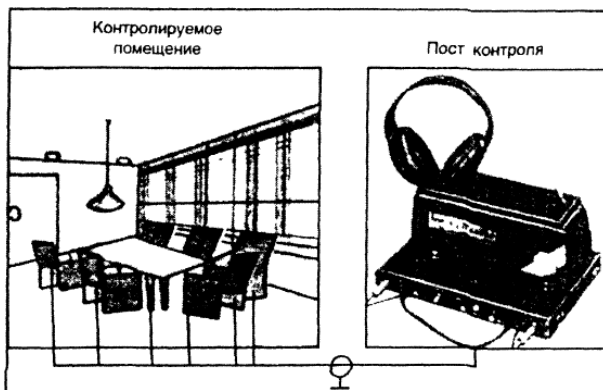


Рис. 81. Стационарный обнаружитель диктофонов RM-200

Устанавливается в служебных помещениях и предназначен для обнаружения магнитного излучения, со здаваемого включенным диктофоном (магнитофоном). Решетка магнитных датчиков закамouflирована в виде брусков, подключенных к устройству обработки сигналов и индикации, которое и указывает номер места за столом, где выявлен работающий магнитофон. Устройство автоматически поддерживает максимальную дальность обнаружения (от 10 до 50 см для различных типов диктофонов) при изменении уровня помех, обладает высокой помехоустойчивостью за счет адаптивной компенсации помех и цифровой обработки сигнала. Обеспечивается одновременный контроль от 2 до 6 рабочих мест, выполнен в виде настольного прибора.

Основные характеристики:

- устройство обработки и индикации — 170x170x30 мм; в масса — 0,5 кг;
- датчик — 230x35x25 мм;
- масса — 100 г;
- индикация — световая, звуковая;
- дальность обнаружения диктофонов (в зависимости от типа) — 10— 50 см.

Используется и портативный, носимый детектор диктофонов типа RM-100 (рис. 82).



Рис. 82

Существенной преградой на пути злоумышленника с подслушивающей техникой является создание на коммерческих объектах особых, защищенных от подслушивания помещений для проведения заседаний, переговоров и конфиденциальных бесед. Таким помещениям присваивается статус специальных, они оборудуются с учетом следующих требований:

- здание, где размещаются такие особые помещения, должно иметь круглосуточную охрану и систему сигнализации;
- помещение располагается, по возможности, в центре здания, рядом с кабинетами руководства коммерческого объекта;
- если в помещении должны быть окна, то желательно, чтобы они не имели балконов и не выходили на соседние с объектом здания, а смотрели бы на внутренний двор или закрывались глухими ставнями;
- внутри помещения должно быть минимальное количество мебели; конструкция мебели должна быть наиболее приспособлена для работы специалиста по поиску техники подслушивания;
- в помещении не должно быть радиоэлектронных устройств, компьютеров, телевизоров, магнитофонов;
- телефонная связь, как наиболее «удобная» для подслушивания, должна осуществляться особым образом, который порекомендует специалист по защите.

Известен и такой способ защиты, как проведение переговоров в прозрачной, оборудованной из оргстекла и пластиков кабине. Это сделано для того, чтобы сразу заметить любой посторонний (непрозрачный) предмет, в том числе и «оставленную» кем-нибудь аппаратуру подслушивания. В такой

кабине все предметы, в том числе и мебель, также сделаны из прозрачных пластиков. Специальная система вентиляции подает воздух внутрь кабины.

При выборе способа защиты помещений следует помнить о том, что эффективность ее будет высокой только при строгом соблюдении режима посещения и работы в таком специальном кабинете. Необходима и периодическая проверка его специалистом по поиску техники подслушивания. Практика показывает, что строгое соблюдение всего комплекса мер безопасности в сочетании с личной заинтересованностью сотрудников в процветании своей фирмы может создавать непреодолимый психологический барьер для злоумышленников и конкурентов, у которых страх быстрого разоблачения их преступных действий на объекте будет сильнее желания получить какие-либо личные выгоды и вознаграждение за установку техники подслушивания.

6.4.2. Противодействие радиосистемам акустического подслушивания [^]

Акустические системы радиоподслушивания (радиозакладки) обеспечивают подслушивание с передачей воспринимаемых разговоров или звуковых сигналов и шумов к злоумышленнику по радиоканалу или по проводам на радиочастотах.

По применению и конструктивным особенностям радиозакладки подразделяются на микрофонные и телефонные. Радиозакладки — это миниатюрные радиопередатчики, работающие, как правило, на частотах УКВ-диапазона для передачи сигналов по эфиру или на частотах 100—150 кГц (для передачи сигналов по проводам). Отличие микрофонных и телефонных радиозакладок заключается в том, что телефонные используют микрофон телефонного аппарата, а микрофонные — свой собственный, встроенный. Кроме того, микрофонные радиозакладки используют собственный источник питания и внешние — типа электросети, а телефонные — питание АТС.

По используемому диапазону радиочастот отмечаются участки 80-170 МГц, 350-500 МГц. По дальности распространения сигналов отмечаются радиозакладки от 100 до 2000 м (см. таблицу 10).

Таблица 10

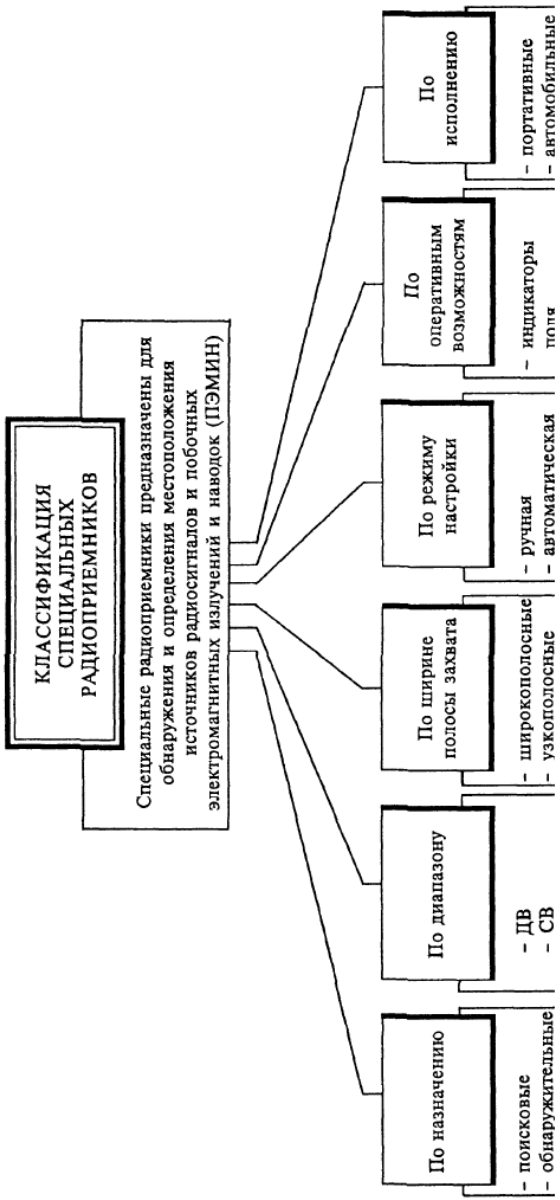
Общие характеристики современных радиозакладок

| | |
|------------------------------|--|
| Используемые диапазоны (МГц) | 88-108; 130-150; 140-170; 378-399; 400-500; 700-750 |
| Дальности связи (м) | 100; 150; 200; 250; 300; 400; 800; 1000; 2000 |
| Мощности (мВт) | 2,5; 3,5; 10; 20; 25; 100 |

Наибольшее распространение получили дальности от 100 до 350 м. Отдельные экземпляры обеспечивают дальность до 500 — 1000 м при диапазоне частот порядка 100— 170 МГц. Основная масса моделей развивает мощность в пределах 10 — 25 мВт.

Основным демаскирующим признаком радиозакладок является наличие радиоизлучения соответствующего диапазона радиоволн. Следовательно, для выявления наличия этих радиосигналов необходимы специальные радиоприемные устройства обнаружения и анализа (рис. 83).

Специальные радиоприемные устройства для поиска и обнаружения радиоэлектронных средств, используемых для проникновения к источникам конфиденциальной информации, характеризуются в основном следующими параметрами:



- целевое назначение;
 - схемное решение;
 - диапазон принимаемых частот;
 - чувствительность;
 - избирательность;
 - точность отсчета частоты принимаемого сигнала;
 - оперативность управления;
 - транспортабельность.

Целевое назначение радиоприемного устройства в значительной степени предопределяет его возможности. Радиоприемники могут предназначаться для поиска, обнаружения, приема, перехвата, пеленгования, измерения характеристик сигналов и других целей. В зависимости от этого к ним предъявляются различные требования по таким характеристикам, как диапазон принимаемых частот, чувствительность и избирательность, точность установки (или определения) частоты принимаемого сигнала, вид модуляции принимаемых сигналов и другим.

Схемное решение приемника обуславливает его сложность и во многом определяет характер его использования. По схемному решению приемники бывают прямого усиления и супергетеродинные, обнаружительные широкодиапазонные и поисковые с автоматической перестройкой частоты, многофункциональные, сканирующие с микропроцессорным управлением и другие системы и комплексы.

Диапазон принимаемых частот выбирается с таким расчетом, чтобы полностью охватить возможные участки спектра частот, используемых для передачи сигналов. Приемники для обнаружения излучения, как правило, широкодиапазонные с непрерывным перекрытием диапазона, например, от 20 до 1800 МГц. Широкодиапазонность позволяет вести поиск и обнаружение сигналов с достаточной вероятностью их выявления при минимальном числе приемников. Узкодиапазонные приемники ориентированы на прием сигналов в определенных участках спектра радиоволн: КВ, УКВ, метровом, сантиметровом и других.

Чувствительность является одним из важных показателей радиоприемника. Она характеризует его способность принимать самые слабые сигналы, поступающие в антенну, и воспроизводить их соответствующим образом на выходе. Количественно чувствительность приемника определяется наименьшим значением

ЭДС или наименьшей мощностью принимаемого сигнала в антенне, при котором на выходе приемника уровень сигнала и соотношение сигнал-шум достигает необходимой величины, обеспечивающей нормальную работу конечных устройств. Чем меньше требуемое значение ЭДС или мощность принимаемого сигнала на входе приемника, тем выше его чувствительность.

Избирательность приемника характеризует его способность выделить полезный сигнал из всех других сигналов, поступающих в приемную антенну одновременно с полезным сигналом и отличающихся от него по своим несущим частотам. В первом приближении избирательность может быть оценена по резонансной характеристике приемника. Резонансной характеристикой приемника называется зависимость его чувствительности от несущей частоты принимаемых сигналов при неизменной его настройке.

Область частот, одновременно пропускаемых приемником, называют полосой пропускания. Полоса пропускания выбирается с учетом назначения приемника. Расширяя полосу пропускания, ухудшают избирательность, и наоборот. На практике противоречивые требования по избирательности и полосе пропускания приемника решаются компромиссно в зависимости от заданных требований.

Точность отсчета частоты определяет возможность приемника дать точное значение частоты принимаемого сигнала. В зависимости от назначения приемника можно определять область частот сигнала, например, порядка 150 МГц, а можно и весьма точно: частота принимаемого сигнала равна 150,43 МГц.

Оперативность управления характеризует способность приемника производить настройку на заданный диапазон и частоту сигнала с минимальной затратой времени. Оперативность управления достигается удобством и простотой управления приемником, наличием минимального количества органов управления.

Транспортability является одним из важных показателей и характеризуется габаритами и весом приемника.

В практике работы служб безопасности в качестве оперативных средств обнаружения радиосигналов закладных устройств широко используются простейшие приемники, получившие название индикаторов поля.

Индикаторы поля

Индикаторы поля или обнаружители сигналов предназначаются для обнаружения радиомикрофонов и телефонных радиозакладок. Индикаторы поля представляют собой приемники прямого усиления, работающие в широком диапазоне радиоволн в бесперестроечном режиме. Большинство моделей индикаторов перекрывает диапазон частот от 20 до 1000 МГц и более. Такое перекрытие по частоте обеспечивается специальной конструкцией и схемным решением, ориентированными на обнаружение электромагнитного поля в непосредственной близости от его источника. Антенна индикатора поля воспринимает высокочастотные электромагнитные колебания, которые посредством гальванической связи прямо передаются на детектор. Пролетектированный сигнал подается на усилитель и далее — на сигнальное устройство оповещения.

Чувствительность индикаторов поля достаточно низкая и лежит в пределах от десятых долей до единиц милливольт (часто в пределах 0,4 — 3 мВ). Естественно, что чувствительность индикатора поля меняется в зависимости от значения частоты, так как в весьма широком диапазоне частот невозможно обеспечить равномерную частотную характеристику на неперестраиваемых элементах приемника. Кроме того, чувствительность приемника определяется еще и действующей высотой антенны. Если в ходе поиска индикатор принимает сигналы из неконтролируемого помещения (т.е. мешающие сигналы), следует уменьшить длину антенны. Прямая гальваническая связь антенны с детектором необходима для приема смодулированных сигналов с АМ, сигналов с ЧМ, которые при их детектировании на амплитудном детекторе на выходе дают постоянный уровень сигнала. На рис. 84 приведена одна из возможных принципиальных схем индикатора поля (ИП).

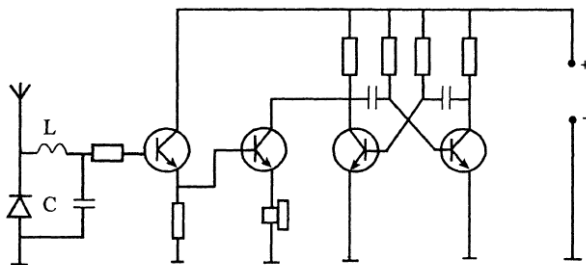


Рис. 84. Принципиальная схема индикатора поля

На схеме L и C составляют фильтр высокочастотной составляющей. Далее низкочастотный сигнал поступает на двухкаскадный усилитель и на сигнализатор, собранный по триггерной схеме.

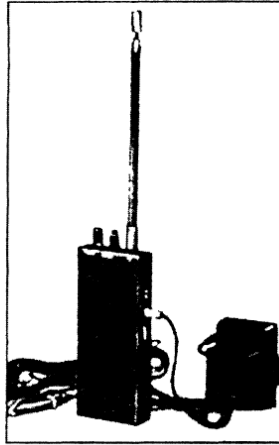
Часто на входе ИП устанавливаются режекторные фильтры на частоты 77, 173, 191 и 215 МГц, подавляющие поступление сигналов мощных вещательных и телевизионных станций.

В таблице 11 приведены основные тактико-технические характеристики распространенных на нашем рынке индикаторов поля.

Таблица 11

Таблица основных ТТХ индикаторов поля

| №№ п/п | Тип (МГц) | Диапазон частот (мВ) | Чувствительность (м) | Дальность обнаружение |
|--------|-----------|----------------------|----------------------|-----------------------|
| 1 | ИП - 1 | 50 - 1200 | 0,4 - 3 | 0,15 - 2 |
| 2 | ИП - 3 | 20 - 1200 | 0,4 - 3 | 0,25 - 2 |
| 3 | ИП - 4 | 25 - 1000 | 0,4 - 3 | 0,15 - 2 |
| 4 | ИПАР | 70 - 1000 | 0,4 - 3 | 0,15 - 4 |
| 5 | АЛЬКОР-М | 45 - 1200 | 100 МКв | ДО 6 |
| 6 | РТ - 022 | 30 - 1000 | - | 0,2 - 25 |
| 7 | RM - 10 | 88 - 100 | 3 | - |
| 8 | D - 026 | 50 - 1000 | 0,5 - 3 | - |
| 9 | КС - 204 | 50 кГц - 1000 кГц | - | - |



*Рис. 85. Индикатор
поля ИП-5*

Панорамные радиоприемники

Специфичность этих приемников заключается в автоматизации поиска в режиме сканирования по частоте. Часто такие приемники снабжаются специальной электронно-лучевой трубкой, позволяющей наблюдать некоторую часть диапазона по сторонам от конкретной контролируемой частоты. Такие приемники получили наименование панорамных. Поиск сигналов радиозакладок в сочетании с обзором в значительной степени облегчает решение задачи выявления их наличия в данном здании, помещении или прилегающей территории.

Панорамное наблюдение радиосигналов не только позволяет отметить наличие сигнала на какой-то частоте, но и определить его спектральный состав и особенности, что позволит достаточно просто отделить разные сигналы от речевого, имеющего специфическую структуру спектра. Кроме того, достаточно четко определяется и вид модуляции — АМ или ЧМ по ширине спектра.

Основными техническими характеристиками панорамных приемников (или сканеров) являются:

- разрешающая способность по частоте;
- точность отсчета частоты;
- полоса обзора;
- скорость обзора.

Например, высокочувствительный носимый сканер «ICOM-IC-R-7100» предназначен для контроля сигналов радиопередающих

устройств в диапазоне от 500 кГц до 1900 МГц.

Его характеристики следующие:

- Все виды модуляций.
- 1000 каналов памяти.
- Выход управления на компьютер.
- Диапазон: 2-30 МГц; 30 МГц— 1,3 ГГц; 1,3-1,9 ГГц.
- Виды модуляции: SSB, AM, NFM, WMF.
- Канальная память: 20 банков по 50 каналов.
- Скорость сканирования: 30 каналов в секунду.
- Питание: 4 элемента типа 316.

Основные характеристики наиболее современных и распространенных на отечественном рынке сканеров приведены в таблице 12.

Широкодиапазонный сканирующий приемник

Предназначен для приема радиосигналов различной модуляции в широком диапазоне частот.

Основными достоинствами приемника являются:

- ввод значения частоты с функциями памяти;
- «шумовая» и «сигнальная» схемы бесшумной настройки (БШН);
- аттенюатор;
- схемы шумоподавителя и автоматической подстройки частоты;
- 900 каналов памяти, программируемых пользователем;
- разнообразные режимы сканирования.

Таблица 12

| Параметры | Тип сканера | | | | | |
|----------------------------------|----------------|---------------|---------------------|----------------|-----------------------------|------------------------------|
| | Тантал 1000 | Uniden 120 | Универс МВТ-7100 | ICOM IC-R1 | AR-3000 | AR-8000 |
| Диапазон частот, МГц | 20-1000 | 29-512 | 0,1-1650 | 0,1-1300 | 0,1-2036 | 0,5-1900 |
| Разрывность диапазона частот | нет | есть | нет | нет | нет | нет |
| Чувствительность, мкВ | 0,3-1,8 | 0,15-0,25 | 0,5-10 | 0,32-6,3 | 0,25-3,0 | 0,25-3,0 |
| Виды демодуляторов | АМ, ЧМ, ШЧМ | АМ, ЧМ | АМ, ЧМ, ШЧМ, ОБП | АМ, ЧМ, ШЧМ | АМ, ОБП, ЧМ, ШЧМ АМПН | АМ, ОБП, ЧМ, ШЧМ, АМПН |
| Скорость сканирования, канал/сек | 14 (50) | 100-300 | 30 | 10-20 | 30-50 | 30 |
| Шаг перестройки по частоте, кГц | 10-50 | 5-12,5 | 1-100 | 0,5-50 | 0,05-999,95 | 0,05-999,95 |
| Кол-во программируемых каналов | 16 | 100 | 1000 | 100 | 400+400 | 1000+1000 |
| Габариты, мм | 200×138×75 | 150×60×40 | 155×65×38 | 102×55×49 | 200×138×80 | 160×65×40 |

Этот радиоприемник может независимо выполнять сканирование в двух различных режимах

IC-R7100 (рис. 87) может комплектоваться:

- сверхширокодиапазонной всенаправленной дисконусной антенной АН-7000;
- внешним громкоговорителем SP-7;
- внешним громкоговорителем IS-SP3;
- внешним громкоговорителем АЧХ SP-20;

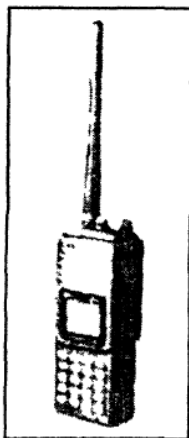


Рис. 86.
Сканер
AR-8000

- телевизионным адаптером TV-R-7100;
- преобразователем уровня CI-V-CT-17 для управления радиоприемником с ПЭВМ;
- ручкой для переноски MB-23;
- кронштейном для установки на автомобиле IC-MB5;
- синтезатором речи VT-6;
- часами всемирного времени GC-5.

Основные характеристики:

- рабочий диапазон — 25- 1999,9999 МГц;
- режимы модуляции — SSB(USB/LSB);
- АМ (обычная и широкополосная), WFM, FM (обычная и узкополосная);
- габаритные размеры — 241х94х239 мм;
- масса — 6 кг.

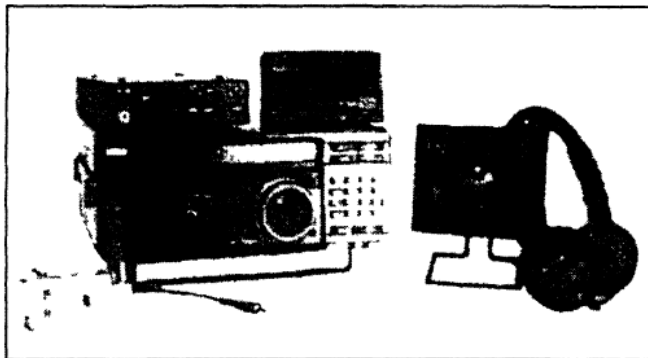


Рис. 87

Для обнаружения радиозакладок, передающих подслушиваемые переговоры по проводным системам, также имеются средства обнаружения. Одним из известных индикаторов электрических сигналов в проводных линиях является индикатор «СКАНЕР-3». Он предназначен для выявления сигналов подслушивающих устройств в силовых, телефонных, радиотрансляционных и других проводных системах (рис. 88).

Основные характеристики:

- Диапазон поиска — от 200 Гц до 7 МГц
- Чувствительность, мкВ:
в диапазоне 200 Гц — 20 кГц — не хуже 100;
в диапазоне 20 кГц — 7 МГц — не хуже 30
- Число поддиапазонов — 5.
- Индикаторы уровня напряжения на входе, В — 5 — 75 и 75-250.
- Питание — 9 В батарея/сетевой адаптер.
- Габаритные размеры—180x80x20.

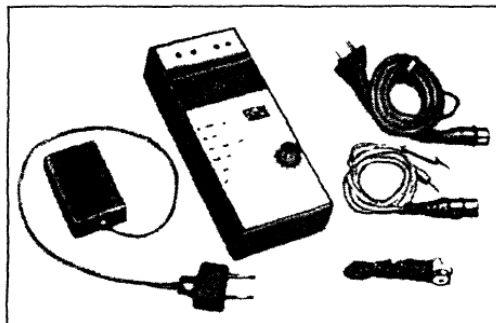


Рис. 88

Нелинейные локаторы

Нелинейные локаторы обеспечивают обнаружение в предметах интерьера и строительных конструкциях помещений технических средств несанкционированного подключения и подслушивания, нелегально установленных (или вмонтированных) в мебель, стены, другие элементы, имеющих в себе полупроводниковые компоненты, электронные и радиовзрыватели, радиомикрофоны, отдельные платы и другие составляющие.

Обнаружение обеспечивается независимо от того, активен или пассивен элемент контроля. Обнаружение осуществляется путем облучения радиоэлектронных устройств высокочастотными импульсами и приема отраженного от них сигнала в режиме непрерывного облучения исследуемых поверхностей. Отраженная энергия в своем составе содержит помимо основной частоты (первой гармонической) вторую, третью и более высокие гармонические составляющие. Если в отраженном сигнале имеются такие, то это свидетельствует о наличии электронных элементов в исследуемой поверхности. Если же нет, то и нет излучающих (отражающих) объемов и поверхностей.

Приемное устройство нелинейного локатора настроено на вторую (реже третью) гармонику и не принимает сигналы первой гармоники.

Тактико-технические характеристики некоторых моделей нелинейных локаторов, имеющих на отечественном рынке средств противодействия несанкционированным действиям, приведены в таблице 13, а внешний вид одного из них на рис. 89.

Характеристики нелинейных локаторов

| № п/п | ТТХ/Тип | НП-5 | НП-5л | Обь-1 | Люкс | Циклон | Энвис | Родник |
|-------|------------------------------------|------|-----------|---------|---------|---------|-----------|---------|
| 1 | Частота сигнала облучения (МГц) | 435 | 885-895 | 1000 | 435 | 680 | 910 | 910 |
| 2 | Частота принимаемого сигнала (МГц) | 870 | 1770-1790 | 2000 | 870 | 1350 | 1820-2730 | 1820 |
| 3 | Длительность импульсов (м/сек) | 0 | 1 | 3 | - | - | - | - |
| 4 | Частота следования импульсов (кГц) | 1 | 300-500 | - | - | - | - | - |
| 5 | Дальность обнаружения (м) | - | 0 | 0,5-2 | - | - | 0,3-3 | 0,5-5 |
| 6 | Мощность излучения | - | - | 250 мВт | 20 Вт | 300 Вт | 200 мВт | 250 мВт |
| 7 | Чувствительность | - | - | -145 дБ | -130 дБ | -120 дБ | - | - |

В качестве примера рассмотрим более подробно технические характеристики одного из нелинейных локаторов.

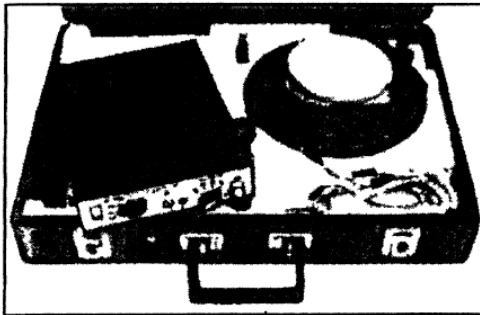


Рис. 89

Нелинейный локатор

Обеспечивает обнаружение в строительных конструкциях помещений и предметах интерьера скрытно установленных радиопередающих устройств и других технических средств съема информации, содержащих в себе полупроводниковые компоненты. Обнаружение осуществляется путем облучения радиоэлектронных устройств высокочастотным импульсом и анализа 2-й гармоники

отраженного сигнала.

Основные характеристики:

- напряжение источника питания — сеть переменного тока (частотой 50 Гц), 198 — 242 В;
- мощность, потребляемая от сети переменного тока, — не более 40 ВА;
- масса изделия в укладочном чемодане без преобразователя и удлинительной штанги — не более 7 кг;
- время непрерывной работы — не менее 8 час;

передатчик:

- несущая частота — 885 — 895 МГц;
- длительность радиоимпульса — не более 3 мкс;
- частота следования радиоимпульсов:
- режим «400 мин» и «400 макс» — 300 — 500 Гц;
- «20 к» — 15-25 кГц;
- импульсная мощность:
- режим «400 мин» — 250 — 400 Вт;
- «400 макс» и «20 к» — 25-40 Вт; 223

приемник:

- реальная чувствительность при соотношении сигнал/шум не менее 6 дБ, при выходном напряжении 100 мВ (амплитудное значение) — не хуже 10-11 Вт.
- динамический диапазон приемника — не менее 15 дБ.

Выявление местонахождения радиозакладки после того, как ее сигнал был обнаружен, возможно как по самому радиосигналу путем пеленгования, так и по физическому проявлению как инородного тела в конструкциях здания, мебели и других предметах.

Для определения места расположения путем радиопеленгования используются специальные радиоприемники, снабженные антеннами с выраженной диаграммой направленности, позволяющие с определенной точностью измерить направление сначала из одной точки, а затем из другой. Пересечение направлений дает на карте точку нахождения источника сигнала.

Обнаружив местонахождение радиозакладки, по ступают по-разному. Можно затеять радиоигру — дезинформацию. Одним из методов введения злоумышленника в заблуждение является передача ложных сведений. Применять этот метод, естественно,

следует, если точно установлено, что переговоры подслушиваются. Дезинформация может иметь успех только при умелой ее организации, проведении продуманных мероприятий, способных ввести злоумышленников в заблуждение и заставить их принимать ложные сведения за действительные.

Последним средством противодействия является физическое изъятие закладки из места ее установки.

Особый случай — посещение злоумышленниками различных мероприятий, исключающее изъятие принесенных радио закладок. В этом случае прибегают к постановке активных радиоэлектронных помех, нарушающих работу системы радиоподслушивания.

Радиоэлектронные помехи — это непоражающие электромагнитные излучения, которые нарушают или затрудняют работу радиолинии «передатчик — приемник». Воздействуя на приемное устройство злоумышленника, помехи искажают, затрудняют или исключают выделение полезного сигнала. Под воздействием помех радиолиния «закладка — приемный пункт» может вообще не работать, несмотря на полную исправность и работоспособность.

В зависимости от способа наведения помех, соотношения ширины спектров помех и полезных сигналов помехи подразделяются на заградительные и прицельные. Заградительные помехи имеют ширину спектра частот, значительно превышающую полосу, занимаемую полезным сигналом, что позволяет его подавлять целиком в полосе частот. Такие помехи можно создавать, не имея точных данных о параметрах сигнала конкретного устройства. Так, например, генератор помех «СФЕРА - 1» перекрывает сплошной заградительной помехой диапазон частот от 300 кГц до 10 ГГц.

Особенностью заградительных помех является то, что при неизменной мощности передатчика помех их спектральная плотность мощности уменьшается по мере расширения спектра излучения.

Прицельные помехи имеют ширину спектра, соизмеримую (равную или в 1,5 — 2 раза превышающую) с шириной спектра подавляемого сигнала. Прицельные помехи характеризуются высокой спектральной плотностью мощности, сосредоточенной в узкой полосе частот.

Любой передатчик помех излучает модулированные высокочастотные колебания требуемой мощности в заданном диапазоне частот. Чаще всего такие передатчики излучают

заградительную помеху в достаточно широком диапазоне частот.

Передатчик помех состоит из источника шумового сигнала, модулятора и генератора несущей частоты. Основными техническими характеристиками передатчика являются: мощность и дальность действия; диапазон частот; диаграмма направленности излучения; вид Модуляции сигнала (АМ, ЧМ, ФМ) и характер помех — прицельная и заградительная.

Мощность передатчика должна быть достаточной для того, чтобы в точке приема помехи превышали или были бы соизмеримы по мощности с сигналом радиозакладки. Это особенно характерно для речевых сигналов, обладающих повышенной помехоустойчивостью, так как на приемной стороне человеческое ухо может различать полезные сигналы даже при наличии достаточно высокого уровня помех.

Диаграмма излучения должна быть круговой, ибо не известно, в какой стороне расположен приемный пункт. Если же выяснено вероятное направление на приемный пункт, возможно использование направленных антенн.

Минимально необходимое отношение мощности помехи P_n и сигнала P_c на входе подавляемого приемника, при котором достигается требуемая степень подавления, называется коэффициентом подавления по мощности K_n ($K_n = P_n/P_c$). Помеха считается эффективной, если ее мощность на входе подавляемого приемника больше полезного сигнала в несколько раз.

В таблице 14 приведены характеристики некоторых типов генераторов помех.

6.4.3. Обеспечение безопасности телефонных переговоров [^]

Проблема защиты телефонных переговоров в условиях широкой телефонизации общества становится весьма актуальной, т. к. злоумышленники широко пользуются подслушиванием и служебных и домашних телефонов. При этом широко используются такие способы, как подключение к телефонным линиям, установка в телефонную линию телефонных радиозакладок, высокочастотное навязывание и другие варианты подслушивания. Наибольшее распространение получает установка телефонных радиозакладок.

В пространственном плане телефонная радиозакладка может быть установлена в помещении, где злоумышленнику нужно

контролировать телефонные переговоры. Для этого телефонная радиозакладка может быть установлена непосредственно в телефонном аппарате, телефонной розетке или подключена в любой точке помещения к телефонным проводам. За пределами помещения телефонная радиозакладка может быть установлена в распределительной коробке и распределительном шкафу здания. Внутри здания особенно уязвим тракт от телефонного аппарата до распределительного шкафа. В этом случае возможна как установка радиозакладок, так и подключение к линии контактными или бесконтактными способом.

Таблица 14

Характеристики некоторых средств постановки активных помех

| Наименование | Диапазон | Мощность | Назначение | Особенности |
|---------------|----------------------------|---------------------------------------|--|--|
| ПНОМ-3 | 10 кГц-1 ГГц | 20 Вт | Маскирование побочных излучений и наводок | - |
| ПНОМ-4 | 20-500 МГц 100-1000 кГц | 5 Вт 4 Вт | Маскирование побочных излучений и защита линий передачи данных | Пространственное зашумление в диапазоне 20-500 МГц Линейное зашумление в диапазоне 100-1000 кГц |
| ПШ-1 | 50-500 МГц | 3 Вт от сети, 1,5 Вт от аккумулят. | Маскирование побочных излучений | Переносной. Питание от сети и аккумуляторов |
| ПШ-2 | 10-1000 МГц | 5 Вт | «_» | Имеет встроенный индикатор поля на диапазон 10-1000 МГц |
| ГПШ-1000 | 0,1-1000 МГц | «_» | Активная защита ПЭВМ | Сертификат Гос-техкомиссии |
| Гш – К – 1000 | 0,1-1000 МГц | «_» | «_» | Бескорпусной, устанавливается в ПЭВМ. Сертификат Гос-техкомиссии |
| СМОГ | 50 Гц-1 ГГц | «_» | «_» | Бескорпусной, устанавливается в ПЭВМ |

| | | | | |
|-----------|-------------|-------|---|---|
| Волна-ЗМД | 1 кГц-1 ГГц | 15 Вт | Маскирование ПЭМИ; подавление радиозакладок | - |
|-----------|-------------|-------|---|---|

От распределительного шкафа до АТС положен многожильный кабель, подключение к которому весьма затруднительно.

Еще одним «слабым» звеном является АТС. На ней возможно подключение и установка радиозакладки непосредственно к той или иной ячейке. Угрожающие ситуации телефонному тракту представлены в виде модели подключения телефонных радиозакладок на рис. 90.

Многообразие возможных ситуаций определяет многообразие мер и способов защиты телефонных разговоров. Очевидно, что обеспечить безопасность телефонного канала связи очень сложно и дорого. Экономически выгоднее воспользоваться устройствами, позволяющими закрыть сообщения, передаваемые по телефонным каналам, или применять организационные меры, обеспечивающие конфиденциальность переговоров.

Простейшими и в то же время крайне важными мерами борьбы с подслушиванием телефонных переговоров являются мероприятия по обеспечению строгой дисциплины ведения телефонных переговоров.

Внешней телефонной связью должен пользоваться ограниченный круг лиц. Никакие частные переговоры из выделенных помещений не допускаются. Наименования организаций, учреждений, должностных лиц, фамилии и другие сведения не должны употребляться в ходе переговоров.

Запрещается передача по телефону распоряжений, отчетов, сведений о составе, состоянии и деятельности организаций и предприятий. При переговорах всегда нужно помнить, что злоумышленник «не дремлет».

К организационным мерам защиты можно отнести планирование прокладки телефонных линий в зданиях и помещениях таким путем, чтобы было удобно их контролировать и трудно использовать возможности подслушивания. Прокладку телефонных линий следует проводить с уменьшением возможного параллельного пробега и перекрещивания друг с другом.

В целях своевременного определения постороннего включения необходимо обеспечить постоянное наблюдение сотрудниками

телефонной службы за состоянием телефонных линий выделенных помещений.

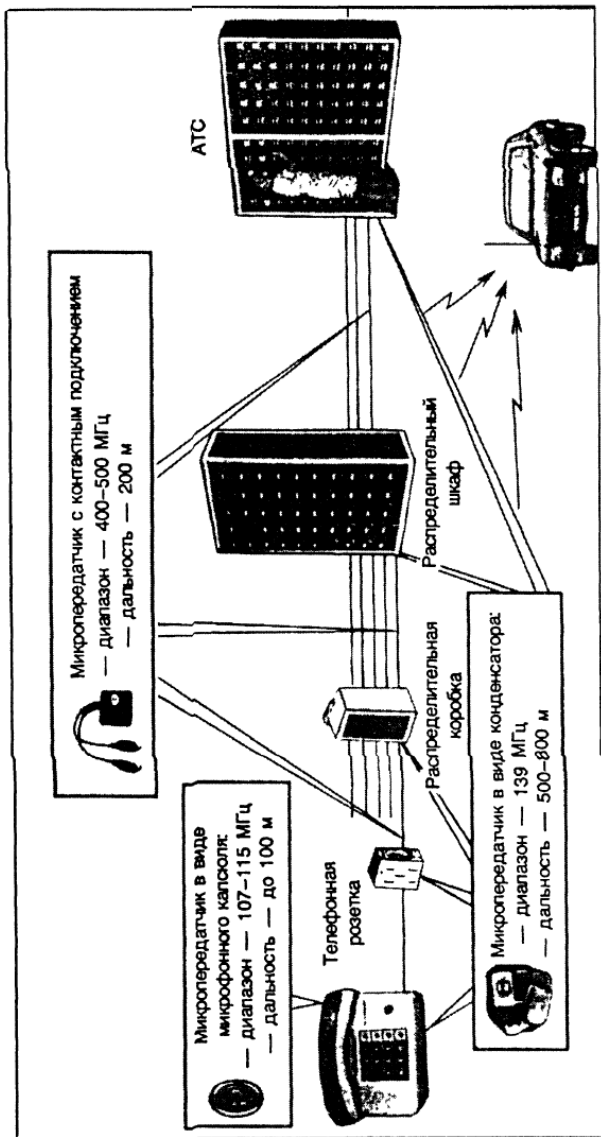


Рис. 90

О всяком изменении слышимости разговора или появлении шумов, тресков, могущих свидетельствовать о включении в линию

подслушивающей аппаратуры, необходимо сообщать в службу безопасности.

Организационной мерой является отключение телефонного аппарата от телефонной линии посредством разъемной розетки на период проведения конфиденциальных переговоров. Это достаточно универсальная мера противодействия от всех вариантов подслушивания. Таким образом просто ликвидируется источник (телефон) подслушивания.

Весьма эффективной мерой противодействия подслушиванию переговоров является использование для ведения конфиденциального общения маскираторов речи или скремблеров. На сегодня техника шифрования речевых сигналов достаточно развита и появилась на рынке в виде удобных переносных или стационарных аппаратов, надежно шифрующих речевой сигнал до его подачи в телефонную линию.

Скремблер — это автономное или встроенное устройство для засекречивания речевой информации, передаваемой по каналам проводной и радиосвязи.

Выбор той или иной модели скремблера зависит от его конкретного применения и характеристик канала связи.

Модели скремблеров, предлагающиеся на отечественном рынке, различаются назначением, конструктивным исполнением и возможностями, а также стойкостью засекречивания, порядком ввода ключа, качеством восстановленной речи, способом электропитания, конструкцией (встроенный или автономный) и другими характеристиками. Присутствуют на нашем рынке и импортные скремблеры. В таблице 15 приведены некоторые типы отечественных и зарубежных скремблеров.

Что нужно учитывать, выбирая тот или иной скремблер? Тут необходимо исходить из того, где можно ожидать установки телефонных радиозакладок. Возможны следующие ситуации.

Ситуация 1. Телефонная радиозакладка установлена в микрофонной трубке. Для защиты конфиденциальных переговоров в этом случае поможет только скремблер — телефонная трубка (рис. 91).

Таблица 15

Характеристики некоторых скремблеров

| № п/п | Тип | Конструкция | Фирма | Основные особенности |
|-------|------------|--|-------------|---|
| 1 | SCR-M12 | Криптофонная приставка | Маском | Защита телефонов и факсов |
| 2 | СТА-1000 | Приставка к телефонному аппарату | — | Защита телефонных переговоров по сетям общего пользования |
| 3 | «Орех» | Телефонная приставка | Анкад | «_» |
| 4 | ASC-2 | Маскиратор накладка на телефонную трубку | «REI» (США) | Автономное кодирующее устройство. Может использоваться с любыми аппаратами таксофоны, радиотелефоны, сотовая связь и др. Защищает как от прямого подслушивания, так и от закладных устройств в телефонных |
| 5 | «Разбег-К» | Абонентский телефонный маскиратор | ПНИЭИ | Защита телефонных переговоров Имеет стаж RS-232 Защищен от микрофонную эффекта и ВЧ-навязывания |
| 6 | «Уза» | Телефонный маскиратор | ПНИЭИ | Размещен в чемодане типа кейс. Подключается к линии напрямую или через акустический соединитель Возможен разговор с пользователем |
| 7 | F-117Л | Скремблер | Маском | Защита переговоров, ведущихся по радиоканалам. Совместим с большинством портативных радиостанций |
| 8 | «Гуман» | Маскиратор | «_» | Предназначен для маскирования телефонных переговоров по абонентским линиям связи. Аппарат включается в разрыв проводов, идущих от телефонного аппарата к микрофонной трубке |
| 9 | «Селена» | Маскиратор-приставка | «_» | Малые габариты и простота подключения к любым телефонным линиям позволяют брать его в деловые поездки |

| | | | | |
|----|-----------------|--|------------|---|
| 10 | Е-24 | Аппаратура закрытия речевой информации | «Алмаз» | Используется с радиостанциями Р-159 м |
| 11 | Е-9к | Аппаратура закрытия речевой и цифровой информации | «Прогресс» | |
| 12 | АГ-2400 | Аппаратура ведения конфиденциальных телефонных переговоров | Анкорт | Выполнен в виде приставки к телефонному аппарату |
| 13 | «Voice changer» | Изменитель голоса | «_» | Предназначен для изменения голоса при телефонном разговоре. Позволяет в широких пределах изменять тембр голоса и делает речь полностью неузнаваемой |
| 14 | Линия-1 | Устройство конфиденциальной связи | «Элерон» | Предназначено для защиты речевой информации в линиях телефонной связи. Используется метод инверсии спектра |
| 15 | «Туман» | Маскиратор телефонных переговоров | «_» | Включается в разрыв проводов микротелефонная трубка — телефонный аппарат |
| 16 | «Угра» | Телефонный скремблер | ПНИЭИ | — |

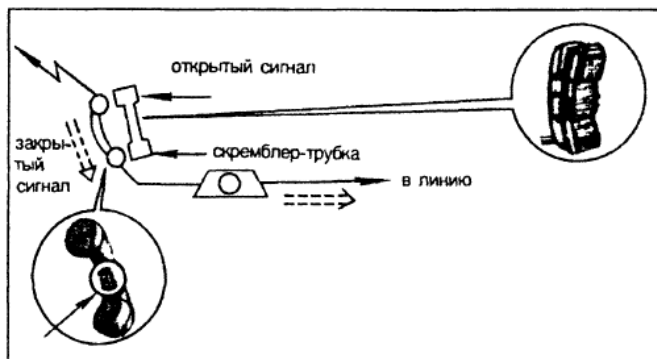


Рис. 91

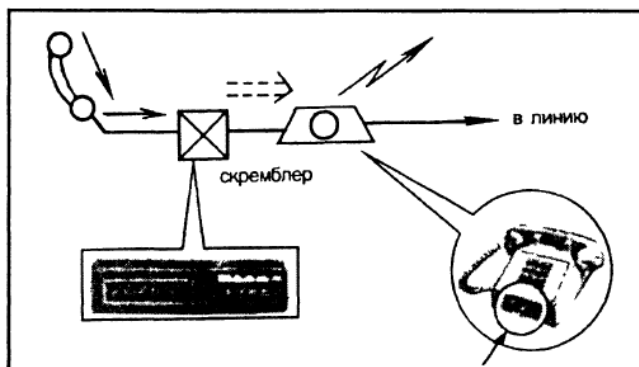


Рис. 92

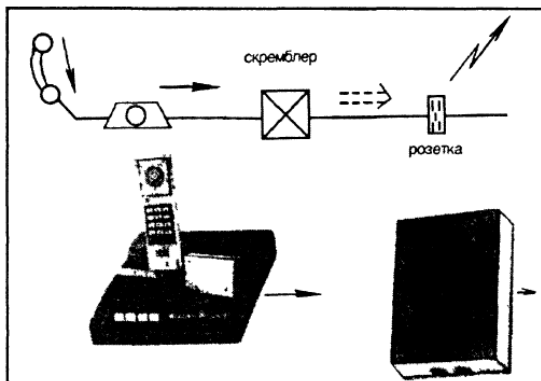


Рис. 93

Ситуация 2. Радиозакладка установлена в корпусе телефонного аппарата. В этом случае скремблер необходимо включать в разрыв проводов микрофонная трубка — телефонный аппарат (рис. 92).

Ситуация 3. Радиозакладка установлена в телефонной розетке контролируемого помещения. В этой ситуации скремблер устанавливается в разрыв проводов между телефоном и телефонной розеткой (рис.93).

Вывод: скремблер устанавливается до возможного (реального) места расположения телефонной радиозакладки, излучающей радиосигнал в эфир.

В обобщенном виде способы противодействия подслушиванию телефонных переговоров представлены в таблице 16.

Таблица 16

Способы противодействия подслушиванию телефонных переговоров

| Способы подслушивания | Способы противодействия | |
|---------------------------------|--|--|
| | Выявления | Противодействие |
| 1. За счет микрофонного эффекта | Специальные измерения телефонных аппаратов на наличие микрофонного эффекта | 1. Замена телефонного аппарата 2. Отключение аппарата от линии 3. Использование специальных устройств защиты |
| 2. Подключение к линии: | | |

| | | |
|--|--|---|
| — контактное | Контроль телефонных линий: — на наличие подключений — на изменение электрических характеристик линии — на изменение напряжения и тока | 1. Прокладка кабеля в защищенных коммуникациях (трубы, кабельные каналы и др.) 2. Непрерывный контроль электрических характеристик 3. Электрическое унитарное подключение средств 4. Использование скремблеров |
| — бесконтактное | Обнаружение мест возможного подключения индукционных датчиков | 1. Использование экранированных кабелей 2. Исключение параллельного прокладывания линий 3. Зашумление линий связи |
| 3. Установка телефонной радиоизлучающей — с передачей сигнала по эфиру | Контроль наличия радиоизлучения при ведении переговоров в диапазоне телефонных частот | 1. Постановка акустических помех 2. Постановка электромагнитных помех 3. Изъятие радиоизлучающей |
| — с передачей сигнала по проводам | Контроль радиоизлучения при ведении переговоров в диапазоне средних волн | 1. Установка в линию подавляющих фильтров 2. Зашумление линий связи акустическими и электромагнитными помехами |
| 4. Высокочастотное навязывание | Контроль наличия радиоизлучения | 1. Постановка электромагнитных помех 2. Установка в линию специальных фильтров высокой частоты |
| 5. Установка дистанционно управляемого микрофона (телефонное ухо) | 1. Контроль элементов телефонной сети 2. Запись на магнитофон сигналов в линии связи за пределами помещения | 1. Постановка активных акустических помех микрофону |

6.4.4. Противодействие лазерному подслушиванию [^]

Совокупность мер по противодействию лазерному подслушиванию можно подразделить на выявление возможных точек расположения лазерного регистратора, обнаружение реальных действий по обеспечению лазерного подслушивания и проведение защитных мероприятий.

Выявление возможных точек расположения лазерного регистратора

При выборе позиции расположения лазерного регистратора злоумышленники решали прямую задачу: определить позицию размещения аппаратуры для подслушивания переговоров. С точки зрения защиты информации необходимо решить обратную задачу: определить возможные (опасные) места расположения лазерного регистратора по отношению к окнам конкретного, выделенного для конфиденциальных переговоров, помещения.

Анализируются варианты выбора позиции:

- направлении, перпендикулярном конкретному окну;
- в направлении горизонтальной плоскости с расположением аппаратуры в разных точках;
- расположение аппаратуры в разных точках и в разных плоскостях.

В каждом из вариантов изучаются расположенные напротив здания, расположение и назначение помещений в возможных точках установки аппаратуры. Особое внимание уделяется рабочим и нежилым вспомогательным помещениям, лестничным переходам, глухим тамбурам и другим местам, которые могут быть использованы злоумышленниками для размещения аппаратуры.

Анализ возможностей злоумышленников начинается с пространственно-азимутальных измерений с учетом требований геометрических законов оптики. Для проведения азимутальных измерений используются различные приборы, такие, в частности, как теодолиты, буссоли и даже лазерные дальномеры. При отсутствии специальных приборов пространственно-азимутальные исследования можно приближенно проводить с помощью обычного прямоугольного треугольника. Треугольник приставляется к окну катетом, а другой катет визируется как перпендикулярная на-

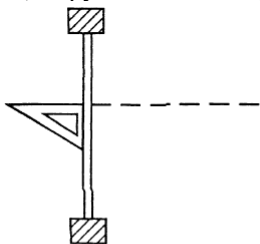


Рис. 94

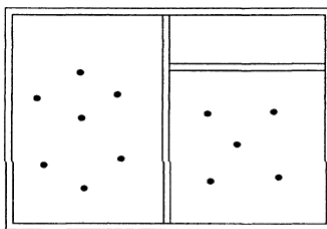


Рис. 95. Возможные точки соприкосновения лазерного луча с окном

правляющая на здания, расположенные напротив защищаемого помещения (рис. 94).

При определении возможной позиции расположения аппаратуры лазерного подслушивания следует исходить из того, что злоумышленник будет направлять лазерный луч не обязательно в центр окна. Он может направлять луч и в отдельные зоны окна с учетом реальной обстановки, исходя из прямой доступности окна (рис. 95, 96).

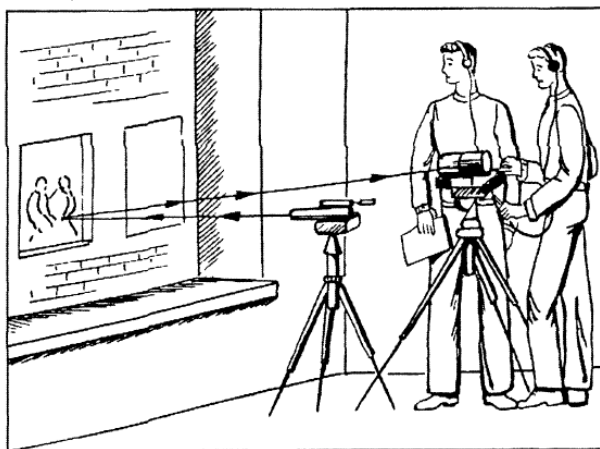


Рис. 96. Вариант пространственно разнесенного расположения лазерного регистратора

Обнаружение

Задачей обнаружения является установление реальных фактов использования лазерных регистраторов для подслушивания конфиденциальных переговоров.

Для целей обнаружения разработаны специальные приборы оповещения о лазерном облучении. Так, норвежская фирма «Симрад» поставляет прибор, сигнализирующий об облучении объектов лазерными средствами. Этот прибор, получивший сокращенное наименование RLI, позволяет обнаруживать лазерное облучение в спектральном диапазоне от 0,66 до 1,1 мкм. Практически все современные лазеры работают на рубине с длиной волны 0,69 мкм; на арсениде галлия с длиной волны 0,84 — 0,89 мкм; на стекле с неодимом и алюмонатриевом гранате — 1,06 мкм. Этот прибор имеет четыре фотоприемника с полем зрения в 135° каждый для кругового обзора в горизонтальной плоскости. Для контроля облучения окна достаточно одного такого фотоприемника. Прибор RLI снабжен акустической и световой

сигнализацией появления облучения. Акустический сигнал тревоги подается длительностью в 1 сек при появлении облучения при одноимпульсном облучении. При непрерывном облучении сигнализация постоянна. Световая сигнализация выдает с помощью светодиода.

Аналогичные сигнализаторы лазерного облучения разработаны в США (LANAWS), Германии (COLDS), Югославии (LIRD), Франции (фирма LTPT).

Находят применение для обнаружения лазерного излучения приборы ночного видения (ПНВ) в пассивном режиме, а также специальные датчики, работающие на эффекте свечения возбужденного ультрафиолетом фосфорного экрана при попадании на его по поверхность с концентрированного лазерного луча.

Защита от лазерного прослушивания

Противодействие подслушиванию конфиденциальных переговоров с помощью лазерных регистраторов речи обеспечивается организационными, организационно-техническими и техническими мерами.

Эти мероприятия следует проводить с учетом особенностей разведывательного контакта, устанавливаемого с помощью лазерного регистратора.

Правоммерно выделить следующие зоны или области проведения защитных мероприятий:

- область собственно выделенного помещения с источниками акустических колебаний;
- собственно оконные проемы как источники передачи колебаний во внешнюю среду;
- область внешней среды.

Все три области составляют элементы разведывательного контакта от источника акустической информации до злоумышленника (рис. 97).

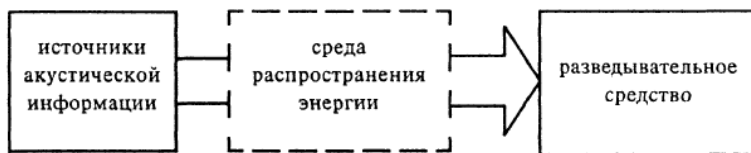


Рис. 97. Модель разведывательного контакта

Чтобы предотвратить несанкционированный доступ к конфиденциальной информации, можно воздействовать на источник, на среду распространения энергии и на средство разведки.

В общем плане защитные мероприятия с учетом выделенных областей разведывательного контакта можно представить следующей матрицей (таблица 17).

Рассмотрим более подробно некоторые из этих мероприятий.

Использование специальных покрытий и специальных стекол предусматривает:

- индофористое покрытие на стеклах — работает по принципу абсолютно черного тела, т. е. поглощает излучение лазера;
- матовое покрытие стекол с высоким коэффициентом поглощения лазерных лучей;
- применение ситалловых стекол. Ситалловые стекла обладают кристаллической поверхностью, рассеивающей падающие лучи. Определенные примеси в составе ситалловых стекол вызывают активную флюоресценцию под воздействием падающих лучей, которая, в свою очередь, создает активную помеху лазерному подслушиванию и является отличным сигнализатором о лазерном облучении.

Таблица 17

Защита от лазерного подслушивания

| Области проведения | Защитные мероприятия | | |
|---------------------------|--|--|---|
| | Организационные | Организационно-технические | Технические |
| Помещение | 1. Использование недоступных для лазерного подслушивания помещений: окна выходят во двор; подвальные, полуподвальные помещения. 2. Расположение рабочих мест, исключаящее прохождение акустических сигналов к окнам | Использование звукопоглощающих облицовок, ковров | Использование средств акустического шумоподавления помещения; ультразвуковые генераторы |

| | | | |
|--------------|--|---|---|
| Окно | Защита окон ставнями, плотными драпировками, специальными экранами | 1. Использование специальных покрытий стекол 2. Применение зеркально-прозрачных пленок | Установка на окна колебательных шайб, создающих активные помехи. Использование окон со стекло-блоками |
| Внешняя зона | 1. Использование зеленых насаждений | 1. Установка светоизолирующих преград: рекламные щиты, транспаранты 2. Использование различных киосков: табачных, газетных и др. | Постановка активных световых (лазерных) помех. |

Средства активной защиты окон представляют собой пьезокристаллические колебательные шайбы и электромагнитные генераторы шумов. Колебательные шайбы приклеиваются к поверхности стекла. К их обкладкам подводится напряжение высокочастотных колебаний от генераторов шума и под его воздействием стекло колеблется с установленной для них частотой. Обычно генераторы шума работают в диапазоне звуковых частот от 10 Гц до 1 кГц. Важно, что подводимая мощность к окну значительно превышает мощность акустического сигнала, достигающего поверхности окна.

Содержание остальных мероприятий не требует специального рассмотрения.

6.5. Противодействие незаконному подключению к линиям связи [^]

Различают два типа линий связи: в атмосфере (радиолинии) и направляющие (кабельно-проводные).

Достоинства направляющих линий связи состоят в обеспечении требуемого качества передачи сигналов, высокой скорости передачи, большой защищенности от влияния посторонних полей, заданной степени электромагнитной совместимости, в относительной простоте оконечных устройств. Недостатки этих линий определяются высокой стоимостью расходов на строительство и эксплуатацию.

По исполнению направляющие линии связи бывают кабельные, воздушные и волоконно-оптические.

Направляющие системы, естественно, могут привлечь внимание злоумышленников как источники получения конфиденциальной информации за счет подключения к ним. Подключение к линиям связи может быть осуществлено контактным (гальваническая связь) и бесконтактным (индукционная связь) путем.

Самым простым способом незаконного подключения является контактное подключение, например параллельное подключение телефонного аппарата, до вольно широко распространенное в быту.

Бесконтактное подключение к линии связи осуществляется двумя путями:

- за счет электромагнитных наводок на параллельно проложенные провода;
- с помощью сосредоточенной индуктивности, охватывающей контролируемую линию.

6.5.1. Противодействие контактному подключению [^]

По физической природе параметры линии связи аналогичны параметрам колебательного контура, составленного из элементов R , L , C . Разница состоит лишь в том, что в контурах эти параметры являются сосредоточенными, а в линиях связи они равномерно распределены по всей длине. Параметры R и L , включенные последовательно (продольные), образуют суммарное сопротивление $Z = R + iwL$, а параметры G и C (поперечные) — суммарную проводимость $Y = G - f iwC$. Из указанных четырех параметров R и C обуславливают энергетические потери, а L и G — волновые изменения в линии связи.

Распространение энергии по линии связи, ток и напряжение в любой точке цепи обусловлены в первую очередь коэффициентом распространения энергии g и волновым характеристическим сопротивлением линии Z_B .

Коэффициент распространения. Электромагнитная энергия, распространяясь вдоль линии связи, уменьшается по величине от начала к концу. Ослабление или затухание энергии объясняется потерями ее в цепи передачи. Следует различать два вида потерь энергии: в металле и в диэлектрике. При прохождении тока по кабельной цепи происходит нагревание токопроводящих жил и создаются тепловые потери энергии. С ростом частоты эти потери увеличиваются: чем больше активное сопротивление цепи, тем

больше потери энергии в металле. Потери энергии в диэлектрике обусловлены несовершенством применяемых диэлектриков и затратами энергии на диэлектрическую поляризацию. Все эти потери учитываются посредством коэффициента распространения.

Любое несанкционированное подключение к линии, последовательное или параллельное, приведет к изменению параметров линии связи. Это и приведет к демаскированию или выявлению такого подключения.

Для выявления контактного подключения к линии связи с целью подслушивания или добывания конфиденциальной информации необходим тот или иной контроль технических параметров линии связи. Режим контроля (постоянный, периодический, разовый) определяется местными условиями и наличием соответствующей контрольно-измерительной аппаратуры.

Действие современных устройств контроля линий связи основано на измерении различных характеристик линии, таких как импеданс (полное сопротивление), сопротивление по постоянному току, напряжение и сила тока. При подключении к линии подслушивающей аппаратуры эти характеристики претерпевают определенные изменения. Обнаружение изменений позволяет принять решение о наличии подслушивания.

Аппаратура проверки проводных линий. По своему назначению и конструктивному исполнению аппаратура проверки проводных линий может быть оперативной и профессиональной.

К оперативным средствам можно отнести анализатор телефонной линии «АТЛ-1» (МПО «Защита информации»). Этот анализатор предназначен для защиты телефонной линии от несанкционированного подключения в нее любых устройств с сопротивлением до 5кОм (рис.98).

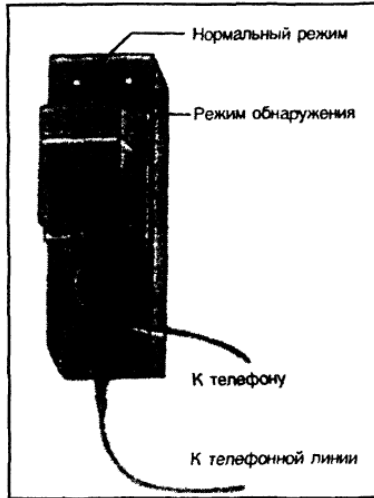


Рис. 98. Анализатор телефонной линии «АТЛ-1»

При подключении прибора к телефонной линии линия считается «чистой» и под такую линию прибор настраивается режим контроля. При несанкционированном подключении к линии загорается красный индикатор (режим обнаружения). При нормальной работе линии горит зеленый индикатор.

Используются и более сложные профессиональные комплексы. Такие, например, как тест-комплект - для проверки проводных линий (рис. 99).

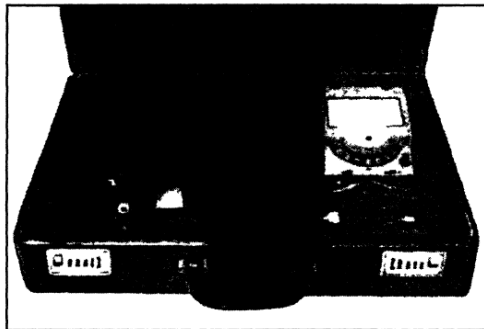


Рис. 99

Такой тест-комплект предназначен для выявления гальванических подключений к любой проводной линии:

- телеграфной и телефонной связи, звукозаписи и воспроизведения;
- переговорных устройств, систем звукоусиления;
- трансляции, сигнализации и пр.

В комплект входят: анализатор, тестер, соединительные провода со щупами, съемные зажимы типа «крокодил», защитное устройство, кейс.

Характеристики:

- максимальная величина тока нагрузки при напряжении зондирующего сигнала 150 В— 1 ма;
- частота зондирующего сигнала — 40 и 400 Гц;
- дальность зондирования — 5000 м.

Зарубежные анализаторы телефонных линий представляют фирмы DYNATEL. Анализатор типа 965 MC представляет собой переносное устройство с микропроцессорным управлением, предназначенное для измерений, диагностики и определения мест повреждений проводников в телефонных кабелях (рис. 100).

Анализатор обеспечивает возможность определения:

- величины напряжения;
- омического сопротивления обрывов — до 100 мОм;
- мест понижения сопротивления изоляции — до 30 мОм;
- величины тока;
- затухания;

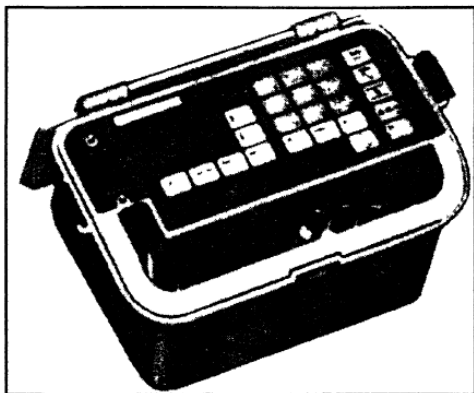


Рис. 100

- шума;
- тонального сигнала;
- а также обнаруживает устройства, которые регулируют

напряжение или ток в линии (REG);

- обеспечивает контроль за абонентской линией, набирает телефонный номер, хранящийся в памяти и предусматривает ручной набор (Dial);

- выбирает тип батареи, режим заряда батареи, опознавание владельца (Auto-Call);

- производит преобразование величин сопротивлений, выраженных в омах, в эквивалентную длину, выраженную в метрах, а также преобразует длину, выраженную в метрах, в величину сопротивления, выраженную в омах.

Обнаружив факт несанкционированного подключения, необходимо установить, где оно осуществлено. Место контактного подключения определяется импульсным методом с помощью импульсных приборов. Импульсный метод основан на использовании явления отражения электромагнитных волн от места подключения к линии подслушивающего устройства. Зная скорость распространения электромагнитной энергии v и время t с момента отправки импульса и возврата его обратно, определяют расстояние до места подключения:

$$L=vt/2$$

Если подключение осуществлено в пределах контролируемой зоны или территории, то используются организационные меры противодействия: изъятие подключенного устройства и защита коммуникаций физическими средствами и мерами.

Если же подключение осуществлено за пределами контролируемой территории, следует принять определенные действия по защите информации:

- не вести конфиденциальные переговоры по этой телефонной линии;

- установить маскиратор речи.

Имеются средства более радикальной борьбы, например электрическое уничтожение (прожигание) подслушивающих устройств, установленных в телефонную линию на участке от АТС до абонентского телефонного аппарата. К числу таких устройств относится генератор импульсов КС-1300. Это устройство работает в ручном и автоматическом режиме. В ручном режиме пользователю дается право выбора момента подачи в телефонную линию сигнала уничтожения подслушивающего устройства. В автоматическом режиме прожигающий импульс посылается в

линию по регламенту с определенной частотой. Устройство обладает следующими техническими характеристиками:

- количество подключаемых телефонных линий — 2;
- временные интервалы, устанавливаемые таймером — от 10 минут до 2 суток;
- мощность прожигающего импульса — 15 Вт;
- потребляемая мощность — 40 Вт;
- питание — сеть 220 В.

В качестве мер защиты внутренних коммуникаций от незаконного подключения необходимо:

- экранирование всех коммуникаций, по которым ведутся конфиденциальные переговоры;
- установка средств контроля мест возможного доступа к линиям связи;
- использование телефонных систем внутреннего использования без их выхода в город и другие меры.

6.5.2. Противодействие бесконтактному подключению [^]

Бесконтактный (индуктивный) съём информации осуществляется путем прикосновения бесконтактного датчика к телефонной линии и прослушивания переговоров на головные телефоны или их записи на магнитофон (рис. 101).

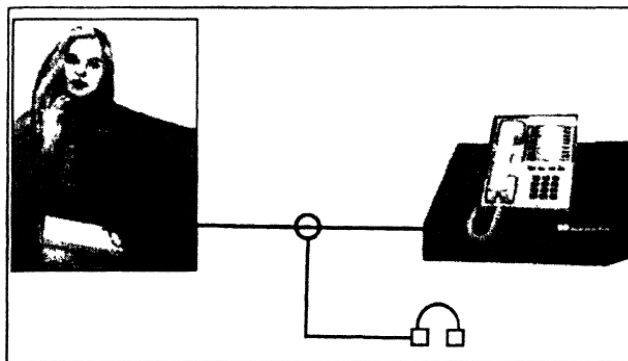


Рис. 101. Вариант бесконтактного съема информации

Индукционный контакт датчика с телефонной линией не вносит никаких изменений в параметры телефонной линии, что весьма ограничивает возможности по обнаружению такого контакта техническими средствами, особенно в том случае, если

телефонная линия не подвергается физическим воздействиям. Если же попытка подключения совершается по отношению к экранированным телефонным линиям, то есть определенные возможности обнаружить бесконтактное подключение приборными средствами. При бесконтактном подключении к экранированным кабелям частично снимается экранирующая оплетка. Этого уже достаточно, чтобы обнаружить повреждение экранного покрытия. Точное определение места повреждения экрана определяется импульсным методом точно так, как это делалось при контактном подключении. Более точно место повреждения определяется подачей в линию звуковых частот и их приемом при движении по трассе кабеля специальным поисковым прибором (рис. 102).

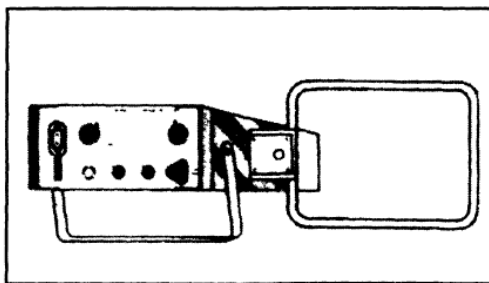


Рис. 102

Этот специальный поисковый прибор предназначен для точного определения места повреждения кабелей связи. Прибор работает совместно с генератором звуковых частот, работающим на частотах 1,03 кГц и 10 кГц. Мощность сигнала генератора звука при работе от встроенных батарей составляет 3 Вт, а при питании от внешней батареи или от сети — 10 Вт. Поиск места повреждения осуществляется проходом по трассе кабеля и определением места излучения звуковой частоты, посылаемой в линию звуковым генератором.

Противодействие бесконтактному подключению осуществляется также организационными и организационно-техническими мерами. В качестве последних рекомендуется использовать генераторы шума и специальные защитные модули. К таким можно отнести универсальный телефонный защитный модуль, способный подавлять индуктивные съёмники, микропередатчики, блокировать автопуски диктофонов. Кроме того, отдельные образцы таких модулей обеспечивают контроль малейших изменений, производимых в телефонных линиях.

Не исключается и посылка прожигающего импульса в линию предполагаемого бесконтактного съема информации.

6.6. Защита от перехвата [^]

Перехват — это способ несанкционированного получения конфиденциальной информации за счет приема электромагнитных сигналов радио диапазона.

Радиоперехват как способ несанкционированного получения конфиденциальной информации обладает определенными особенностями:

- осуществляется без непосредственного контакта с объектом криминальных интересов;
- охватывает большие расстояния и пространства, пределы которых определяются особенностями распространения радиоволн различных диапазонов;
- обеспечивается непрерывно в разное время года и суток и при любой погоде;
- обеспечивает получение достоверной информации, поскольку она исходит непосредственно от источника;
- позволяет добывать самую различную информацию статистического и оперативного характера;
- дает интересующую информацию в реальном масштабе времени и зачастую в виде упреждающих событий (приказы на проведение тех или иных действий);
- осуществляется скрытно; источник информации, как правило, не в состоянии установить факт несанкционированного доступа.

Источниками излучения радиоволн различных диапазонов являются:

- средства радиосвязи, предназначенные для обеспечения мобильной и стационарной систем, в том числе спутников, радиорелейных и других;
- средства сотовой радиосвязи;
- средства пейджинговой связи;
- средства оперативной служебной радиосвязи;
- сигналы радио телефонных удлинителей;
- сигналы радиомикрофонов;
- сигналы технических средств и систем (радиолокационные, радионавигационные системы, сигналы средств электронно-вычислительной техники и пр.);

- другие системы открытого излучения радиосигналов связного или технологического характера (например, средств обеспечения полетов самолетов, средств спасания на водах и пр.).

В качестве примера возможности установления информационного контакта между средствами злоумышленника и источниками радиосигналов рассмотрим частную модель радиоперехвата (рис. 103).

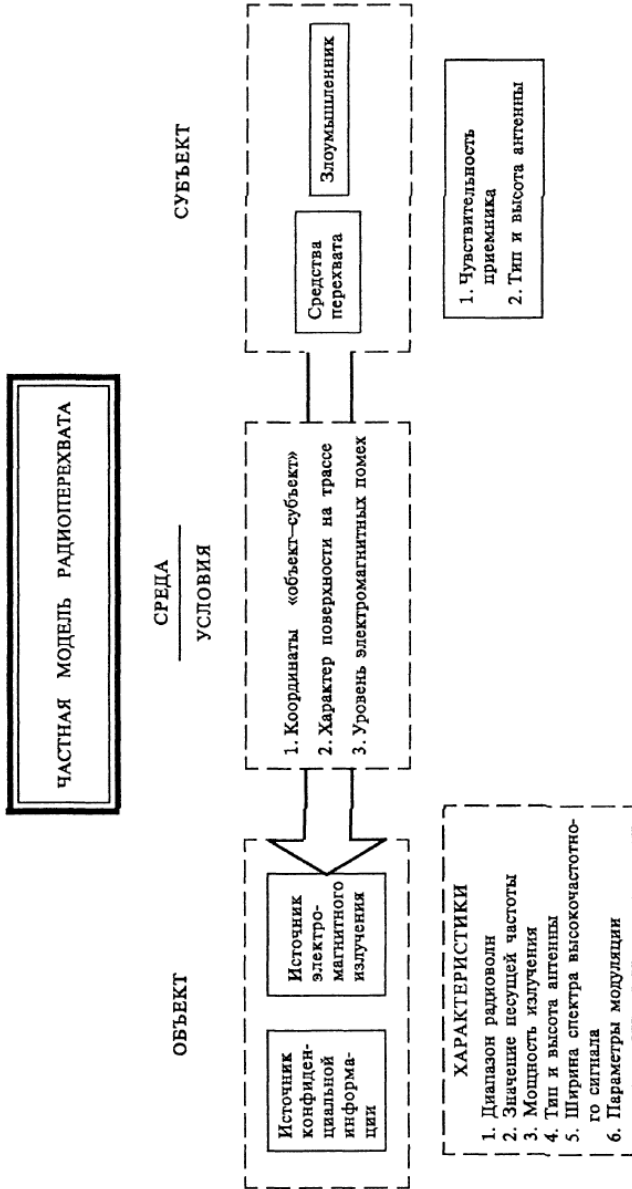


Рис. 103

Модель содержит общие характеристики источника радиосигналов, определяющих возможную дальность их

распространения в пространстве, среду распространения радиоволн и условия, влияющие на ее характеристики и средства злоумышленника, предназначенные для приема радиосигналов.

Соблюдение баланса характеристик объекта, условий, среды и параметров средств разведки позволяет установить информационный контакт и зафиксировать необходимые характеристики источника. Имея определенные методики, можно рассчитать возможность установления такого контакта в конкретных условиях. Условия установления информационного контакта рассмотрим для случая перехвата информации средствами радиоэлектронной разведки. Для этого воспользуемся параметрической моделью такого информационного контакта (рис. 104).

Возможность установления информационного контакта выражается вероятностью R_0

Определить вероятность перехвата электромагнитного сигнала средствами злоумышленника можно с помощью следующей формулы:

$$R_0 = \exp \left(-\frac{k}{1 + q} \right),$$

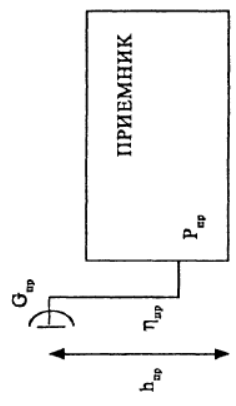
где k — коэффициент размерности ($=7$);
 q — отношение мощности сигнала к мощности шума в точке приема.

Значение q определяется из формулы

$$q = \frac{7 \cdot 16 \cdot 10^{-3} \cdot P_{\text{и}}}{f_c^2 \cdot \Delta f_c} \cdot 10^{10,1 (G_{\text{и}} + G_{\text{с}} - N_0 + Z_0)},$$

где $P_{\text{и}}$ — мощность источника сигнала;
 f_c — несущая частота;
 Δf_c — ширина спектра сигнала;
 $G_{\text{и}}$ — коэффициент усиления антенны источника;
 $G_{\text{с}}$ — коэффициент усиления антенны приемника злоумышленника;
 N_0 — спектральная плотность мощности шумов на входе приемника;
 Z_0 — ослабление радиоволн в среде распространения при заданных условиях.

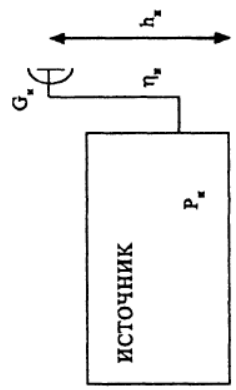
ПАРАМЕТРИЧЕСКАЯ МОДЕЛЬ ИНФОРМАЦИОННОГО КОНТАКТА
СРЕДСТВАМИ РАДИОЭЛЕКТРОННОЙ РАЗВЕДКИ



- $P_{пр}$ — чувствительность
- $G_{пр}$ — коэффициент усиления антенны
- $\Pi_{пр}$ — КПД антенны
- $h_{пр}$ — высота антенны
- N_0 — спектральная плотность шумов

СРЕДА

- Поглощение — Z
- Ослабление — V
- Интерференция
- Рефракция
- Условия
- 1. Время года
- 2. Время суток
- 3. Географическое расположение



- $P_{и}$ — мощность
- $G_{и}$ — коэффициент усиления антенны
- $\Pi_{и}$ — КПД антенны
- $h_{и}$ — высота антенны
- f_c — частота сигнала
- Δf_c — полоса частот сигнала

Рис. 104

Пример. Определить вероятность перехвата электромагнитного сигнала портативными средствами злоумышленника при соотношении сигнал/шум $q = 4,5 \cdot 10^8$.

$$R_0 = \exp\left(-\frac{7}{1+q}\right) = \exp\left(-\frac{7}{1+4,5 \cdot 10^8}\right) = > 0.$$

Следовательно, $K = e^{-0} = 1$.

При этих условиях вероятность перехвата сигнала равна 1, т. е. сигнал может быть уверенно принят средствами злоумышленника.

Подобное описание энергетических и пространственных соотношений, положенных в основу расчетов, приводится в специальной литературе и соответствующих методических и нормативных материалах.

Дальность действия линии разведывательного контакта «Передатчик источника — приемник злоумышленника» определяется энергией (мощностью) передатчика и может быть рассчитана с помощью следующей формулы:

$$D_{\max} = \sqrt{\frac{P_{\text{пер}} \cdot G_{\text{пер}} \cdot G_{\text{пр}} \lambda^2 \eta}{(4\pi)^2 \delta_{\min} R T_{\Sigma} \cdot \Delta f \cdot L}},$$

где: $P_{\text{пер}}$ — мощность передатчика;
 $G_{\text{пер}}$ — коэффициент усиления антенны передатчика;
 $G_{\text{пр}}$ — коэффициент усиления антенны приемника;
 λ — длина волны передатчика;
 η — коэффициент потерь в среде распространения;
 f — полоса сигнала;
 L — коэффициент запаса на неучитываемые факторы (обычно лежит в пределах 3... 10);
 δ_{\min} — минимально допустимое превышение сигнала над шумом по мощности;
 R — постоянная Больцмана;
 T_{Σ} — суммарная шумовая температура на входе приемника.

Дальность перехвата сигналов ПЭВМ можно охарактеризовать такими показателями, учитывающими конструктивные особенности дисплея и антенных систем злоумышленника (таблица 18).

Таблица 18

| Характеристика антенны злоумышленника | Конструкция корпуса АЭВМ | |
|---------------------------------------|--------------------------|---------------|
| | пластмассовый | Металлический |
| Ненаправленная | 50 м | 10 м |

| | | |
|--------------|--------|-------|
| Направленная | 1000 м | 200 м |
|--------------|--------|-------|

Математические расчеты могут быть подкреплены конкретными действиями по определению реальной возможности установления информационного контакта путем приема сигналов своих средств специальными приемными устройствами с изменением расстояний приема и азимутных направлений их расположения. Используя измерители сигналов, можно составить графики уровня излучаемых сигналов в конкретных условиях на конкретной местности.

Результаты математических расчетов и экспериментальных инструментальных измерений позволят четко определить опасность тех или иных сигналов в условиях конкретного их расположения на местности.

Методы защиты от перехвата в общем плане приведены на рис. 105.

Выводы

Опыт работы отечественных и зарубежных специальных служб и служб безопасности предпринимательства позволяет утверждать:

1. Доступ к источникам конфиденциальной информации является весьма серьезной угрозой информационной безопасности различным органам, фирмам, гражданам и предприятиям.
2. В практике промышленного шпионажа для получения интересующей злоумышленников информации находят широкое применение самые различные способы получения конфиденциальной информации, особенно с помощью технических средств несанкционированного доступа к охраняемым секретам, разрабатываемые на основе самых последних достижений науки и техники.

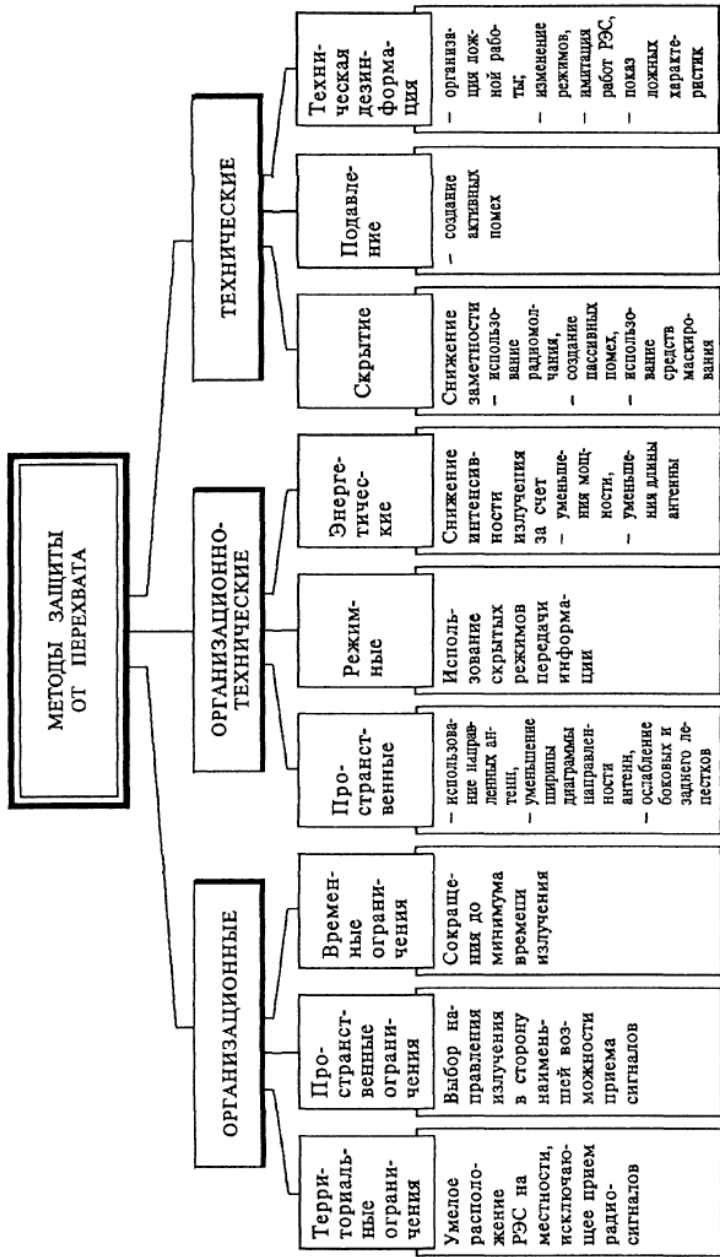


Рис. 105

3. Противодействие несанкционированному доступу к источникам конфиденциальной информации требует создания сложной и четко организованной системы противодействия. Здесь важным является принцип: оружие защиты должно быть адекватным оружию нападения.

Глава 7. КОНФИДЕНЦИАЛЬНОСТЬ ПРИ РАБОТЕ С ЗАРУБЕЖНЫМИ ПАРТНЕРАМИ [^]

7.1. Направления взаимодействия с зарубежными партнерами [^]

7.1.1. Научно-техническое сотрудничество с зарубежными партнерами [^]

В настоящее время бесспорен тот факт, что результаты созидательной интеллектуальной деятельности (новые технические и технологические решения, разработки, «ноу-хау» и т. д.) коллектива специалистов или отдельного исследователя, разработчика являются товаром, который может быть продан, куплен, обменен и украден.

На сегодняшний день самые выгодные виды интеллектуального товара, которые достаточно широко продаются и покупаются — это программные продукты: программы, пакеты прикладных программ, системное программное обеспечение. Это связано с бурными темпами компьютеризации общества. Второе место занимают технологии — с целью их продажи создаются специальные биржи; затем — изобретения, «ноу-хау», материалы экспертных оценок, банки и базы данных. Продажа и покупка остальных видов интеллектуального товара осуществляется нерегулярно, хотя в зарубежной практике дело обстоит иначе, например, достаточно перспективная научно-техническая идея может быть украдена и в короткое время реализована в конкретном материальном продукте.

В последние годы наблюдается активизация международного научно-технического сотрудничества. Участвуя в различных формах международного разделения и кооперации труда, российские предприниматели заключают многочисленные контракты, соглашения, договора. Выборочный анализ последних свидетельствует об отсутствии у российской стороны необходимых знаний и опыта по их составлению, в том числе в части вопросов, связанных с интеллектуальной собственностью. Результатом этого являются существенные экономические потери российской сторо-

ны, которые находят свое конкретное отражение в:

1. потере всех прав, в том числе и патентных, вне территории стран СНГ (а иногда и на этой территории) на интеллектуальную собственность, впервые созданную или доведенную до практики при выполнении контракта (договора, соглашения);
2. в безвозмездной передаче в процессе выполнения соглашения принадлежащей ей интеллектуальной собственности;
3. блокировании процесса дальнейшего создания и коммерческого использования усовершенствований, самостоятельно разработанных ею после окончания срока действия контракта, соглашения, договора;
4. крайне заниженной цене контракта;
5. невозможности защитить принадлежащие российской стороне права в соответствии с российским судопроизводством.

Это происходит вследствие:

1. отсутствия учета специфики российского рынка научных подрядчиков, представляющих собой, в основном, государственные научные организации с государственным финансированием, а следовательно, роли регулирования соответствующих отношений собственности со стороны правительства России;
2. использования только положений законодательных актов страны-партнера при отсутствии ссылок на соответствующие положения российского законодательства;
3. нарушения ряда положений российского законодательства, относящихся, в частности, к процедурам зарубежного патентования, экспортного контроля, договорным отношениям, недействительности договоров и т. д.;
4. отсутствия учета приносимого в процесс взаимодействия собственного интеллектуального вклада российской стороны;
5. чрезмерно широкого определения понятий «предмет соглашения», «изобретение», «право на использование», «совместный» и «собственный» (проприетарный) результат и других;

6. декларации действительности только иностранного текста контракта, а зачастую в отсутствии или неправильном переводе на русский язык раздела контракта, посвященного интеллектуальной собственности;
7. неучтенной стоимости передаваемых российской стороной патентных прав;
8. отсутствия механизма выявления нарушителей прав на объекты интеллектуальной собственности и мер, направленных на пресечение этих нарушений;
9. невыполнения ряда положений межправительственных соглашений в части, касающейся интеллектуальной собственности.

Игнорирование вышеперечисленных аспектов может привести к конфликтным ситуациям, подорвать доверие к процессу эффективного и взаимовыгодного сотрудничества.

Составление соглашений (договоров) о сотрудничестве

Одним из аспектов является правильное составление соглашений о совместном сотрудничестве, где необходимо точно определить тип соглашения (договора), которое имеет первостепенное значение, т. к. из него вытекают отношения сторон к правам на владение интеллектуальной собственностью. Преобладающими формами научно-технического взаимодействия между российскими и зарубежными организациями в настоящее время являются соглашения о научно-техническом сотрудничестве и договоры подряда.

Между этими формами на практике неспециалисту трудно провести четкую грань. В ряде случаев они выступают как крайние формы правового взаимодействия партнеров, между которыми возможны самые различные варианты.

Для соглашений о научно-техническом сотрудничестве характерно согласованное выполнение программы научно-исследовательских, проектно-конструкторских и экспериментальных работ в *целях* достижения единого результата. По своему содержанию обязательства сторон в соглашениях о сотрудничестве — это взаимные обязательства по выполнению исследовательских и научно-технических работ.

Важнейшим условием соглашения о сотрудничестве является наличие у партнеров общей хозяйственной цели (совместной

деятельности по созданию и использованию результатов работы.) Поэтому обязательства сторон в соглашениях о сотрудничестве не противостоят друг другу, а являются общими, едиными.

Для договоров подряда характерно, что одна сторона (подрядчик) за установленную договором плату обязуется выполнить по заказу другой стороны (заказчика) определенные в договоре подряда научно-технические работы и передать заказчику их результаты или оказать услуги научно-технического характера. У каждой из сторон такого договора имеются собственные (несовпадающие) интересы, в связи с чем их обязательства носят встречный, противостоящий друг другу характер.

Отражение в соглашениях вопросов интеллектуальной собственности

1) Интеллектуальная собственность в договорах подряда. Поскольку при проведении заказных работ творческий вклад в результирующую информацию вносится только одной стороной (подрядчиком), выполняющей работу за счет другой стороны (заказчика), в договорах подряда, как правило, не возникает совместных прав на владение объектами интеллектуальной собственности. Охранные документы в этом случае приобретаются либо на имя подрядчика, либо на имя заказчика. Определяющими критериями на практике выступают интеллектуальный и финансовый вклады сторон в создание интеллектуальной собственности.

Независимо от того, на чье имя выданы охранные документы на объекты интеллектуальной собственности, патенты на изобретения, свидетельства на полезные модели и т. д., каждая из сторон имеет определенные права на использование интеллектуальной собственности, полученной в ходе выполнения подрядных работ.

2) Интеллектуальная собственность в соглашениях о сотрудничестве. Полученные в ходе выполнения соглашений о сотрудничестве результирующая информация, результирующий патент, результирующее программное обеспечение, как правило, являются совместной (долевой) собственностью сторон. Доли участников долевой собственности устанавливаются соглашением сторон, а при его отсутствии признаются равными. Соглашением участников долевой собственности может быть установлен порядок определения и изменения их долей в зависимости от вклада

каждого из них в образование и приращение общей собственности*.

В соглашениях о сотрудничестве особое внимание следует уделить вопросам распределения прав на результаты работ, полученные в рамках сотрудничества каждой из сторон, но не являющиеся конечным результатом сотрудничества, так называемые промежуточные результаты сотрудничества.

Анализ мировой практики заключения соглашений в области международного научно-технического сотрудничества показывает, что большинство соглашений предусматривает, что каждая из сторон имеет право на неограниченное использование промежуточных результатов работ на территории своей страны. Для передачи таких результатов в третьи страны требуется согласие всех сторон соглашения. Доходы при этом распределяются между сторонами пропорционально зафиксированной в соглашении доле их участия.

Защита интеллектуальной собственности

Защита прав на совместные объекты интеллектуальной собственности от нарушений третьими лицами должна осуществляться сторонами совместно либо по согласованию с партнером той стороной, которая вела работу по получению правовой охраны в стране, где нарушены соответствующие права.

Меры по защите нарушенных третьими лицами прав на собственные изобретения в стране партнера, созданные сторонами в ходе сотрудничества и переданные друг другу для использования, должны быть четко определены в соглашении о сотрудничестве или договоре подряда. На практике возможны следующие варианты:

1. меры по защите нарушенных третьими лицами прав предпринимаются той стороной, которой такие права принадлежат;
2. меры по защите нарушенных третьими лицами прав предпринимаются обеими сторонами;
3. меры по защите нарушенных третьими лицами прав предпринимаются тем партнером, в стране которого произошло нарушение указанных прав, ибо он обладает большими возможностями по организации защиты в своей стране.

Аналогичным образом в соглашении следует определить

процедуру защиты в случае предъявления в стране партнера претензий или исков со стороны третьих лиц.

Соглашения и договоры подряда рекомендуется готовить на двух языках: русском и языке иностранного партнера, сделав специальную оговорку в соглашении или договоре о том, что каждый из текстов имеет одинаковую юридическую силу.

7.1.2. Научно-техническое сотрудничество. Технологически и обмен и его регулирование. [^]

Научно-техническое сотрудничество — это процесс создания знаний и технологий, обмена ими, процесс, в котором результаты научно-технической деятельности выступают как специфический товар, имеющий потребительскую стоимость. Он разделяется на товар нематериальный: знания, навыки, методы; и материальный: оборудование, инструменты, оснастка и другое. Процесс обмена знаниями и технологиями формирует в самом общем виде рынок технологий с присущим ему инструментариум рыночных отношений.

Объектами научно-технического сотрудничества и технологического обмена являются патенты на изобретения, промышленные модели и полезные образцы, «ноу-хау» (производственный опыт и знания), услуги (инжиниринг), техническая документация, техническая помощь, а также оборудование, машины и другая техника и технологии, в которых материализованы научно-технические знания.

В Российской Федерации в настоящее время действует пакет законов, регулирующих обмен технологиями и соответствующих аналогичным законам ведущих стран мира: Патентный закон; Закон «О товарных знаках, знаках обслуживания и наименования мест происхождения товаров»; Закон «О правовой охране программ ЭВМ и баз данных»; Закон «О правовой охране технологий интегральных схем» (приняты на Пятой сессии Верховного Совета Российской Федерации 23 сентября 1992 г.).

Патентный закон РФ регулирует правовую охрану изобретений и промышленных образцов, при этом введена единая форма охранного документа — патент на изобретения и промышленные образцы и свидетельство на полезную модель.

Постановлением Правительства РФ от 12 июля 1993 г. № 648 установлен порядок использования изобретений и промышленных образцов, охраняемых действующими на территории Российской

Федерации авторскими свидетельствами на изобретения и свидетельствами на промышленный образец, и выплаты их авторам вознаграждения. Постановление распространяется на ранее выданные свидетельства СССР и устанавливает, что юридические лица, независимо от форм собственности, и физические лица, занимающиеся предпринимательской деятельностью, используют изобретения и промышленные образцы, охраняемые действующими на территории Российской Федерации авторскими свидетельствами СССР на изобретение и свидетельствами СССР на промышленный образец, без специального на то разрешения.

Учитывая необходимость сохранения и развития научно-технического потенциала и более широкого использования достижений науки и техники для структурных преобразований экономики России, государственное регулирование технологического обмена расширяет инструментарий стимулирования разработки и использования изобретений, промышленных образцов и полезных моделей за счет механизма льготного налогообложения и других льгот владельцам охраняемых документов. В частности, разработаны методы учета нематериальных активов (изобретений, полезных моделей и других видов творческой деятельности), а также оценки интеллектуальной собственности в рамках сотрудничества (как правило, совместной деятельности) и перенесения их стоимости на издержки по совместной деятельности, что предполагает освобождение от налогов суммы общих затрат на совместную деятельность по доведению, к примеру, изобретения до конечного результата, оговоренного в документе, регулирующем сотрудничество (договор, контракт, соглашение).

Рынок технологий

Как и любой другой, рынок технологий имеет свою структуру, основными элементами которой являются товар, его производство и потребление, а также физические и юридические лица как субъекты рыночных отношений.

Особенность технологии состоит в том, что она может выступать в качестве товара только в случае, если ее владелец обладает исключительным правом собственности на нее. Если же знания, лежащие в основе новой технологии, широко известны, то возможности получения коммерческих преимуществ от ее реализации отсутствуют, и, следовательно, становится

невозможным и получение дополнительной прибыли. Поэтому охрана права интеллектуальной собственности является неотъемлемым элементом рынка технологий.

Международный технологический обмен играет существенную роль в современных мирохозяйственных связях. Это связано с тем, что развитие науки и техники, которое лежит в основе производства новых знаний, имеет глобальный характер, и знания легче, чем любой другой товар, пересекают национальные границы.

В соответствии с методологией ООН, технология подразделяется на высокую, среднюю и низкую. Наиболее мощным коммерческим потенциалом обладает высокая технология. Обмен ею приходится преимущественно на промышленно развитые страны. Средняя и низкая технологии для рынков этих стран практически не представляют коммерческой ценности, так как они широко распространены и их внедрение в большинстве случаев не создает условий для получения дополнительной прибыли.

Средняя и низкая технологии обладают коммерческим потенциалом на рынках развивающихся стран, так как на уровне их научно-технического и экономического развития они обладают «новизной». Однако фирмы этих стран, освоив свои национальные рынки, сталкиваются с серьезными затруднениями при попытках экспорта своей продукции, произведенной на основе этих технологий. Поэтому поток технологий по мере их старения направлен из более развитых к отстающим в своем развитии странам. Российским импортерам зарубежных технологий следует особенно внимательно относиться к оценке коммерческого потенциала приобретаемой технологии не только для внутреннего рынка, но и для будущего экспорта продукции, производимой с использованием этих технологий. Вместе с тем при продаже российских технологий за рубеж следует уделять особое внимание правильному выбору формы и способа передачи технологии. Ошибки в этой области ведут не только к существенным коммерческим потерям, но и к утрате научно-технического приоритета, лидерства в перспективе на мировых рынках.

Участником технологического обмена может быть любое физическое или юридическое лицо, как индивидуальное, так и коллективное (объединения, компании, фирмы, товарищества и ассоциации), а также любые их сочетания, независимо от того, кем они были созданы, кому принадлежат, кем контролируются (государством, правительственными учреждениями, юридическими

лицами или отдельными гражданами), где функционируют, и независимо от форм собственности.

Под потребителем технологии подразумевается сторона, которая получает право (лицензию) на использование или эксплуатацию технологии, носящей патентный или не патентный характер, покупает или каким-либо иным образом приобретает технологию или право на нее.

Под поставщиком технологии подразумевается сторона, которая предоставляет, продает, передает или каким-либо иным образом поставляет технологию, носящую патентный или не патентный характер, или право на нее.

Существует несколько путей технологического обмена. Наиболее распространено разделение потока технологического обмена на коммерческие и некоммерческие, международные, внутригосударственные и внутрифирменные варианты передачи технологии.

К некоммерческим вариантам технологического обмена относятся:

- свободное распространение научно-технической информации (научно-технической, учебной литературы, справочников, обзоров, стандартов, описаний патентов, каталогов, проспектов и т. д.);
- обмен информацией в ходе международных конференций, сессий, симпозиумов и выставок;
- научный обмен, обучение и стажировка ученых и специалистов на бесконтрактной основе или на условиях паритетного возмещения расходов сторонами.

По каналам некоммерческого обмена чаще всего проходит передача технологий в области научных исследований фундаментального характера.

Обмен технологией по некоммерческим каналам обычно сопровождается небольшими расходами, в том числе валютными. Он может осуществляться как по государственной линии, так и частным образом на основе личных контактов.

Передаче технологий прикладного характера больше соответствуют коммерческие каналы, по которым в форме сделок осуществляются:

- продажа или предоставление по лицензии всех форм промышленной и интеллектуальной собственности;
- передача «ноу-хау» и технического опыта в виде технико-экономических обоснований, планов, диаграмм,

моделей, образцов, инструкций, руководств, формул, сборочных или рабочих чертежей, спецификаций, технологической оснастки и инструмента, услуг консультантов и подготовки кадров;

- передача технических знаний, необходимых для монтажа, эксплуатации предприятий, цехов и оборудования, а также проектов по строительству объектов «под ключ»;
- предоставление технологических знаний в рамках соглашений о совместной научно-технической деятельности, совместном производстве и сбыте; контрактов на приобретение и монтаж машин, оборудования, полуфабрикатов или сырьевых материалов или их аренду (лизинг).

На рынке технологий действует сеть покупателей и продавцов, соединенных посредническими звеньями инновационной инфраструктуры. В обобщенном виде она складывается из следующих элементов:

- исследовательских, внедренческих и инновационных форм и компаний, университетов и учреждений, предлагающих результаты своих разработок;
- бирж, торговых домов, ярмарок, аукционов, магазинов и других мест совершения сделок, которые специализируются на определенных видах продаваемых знаний;
- посреднических компаний, предоставляющих профессиональные услуги продавцам и покупателям технологии (инжиниринговых, консультационных, аудиторских, лизинговых, информационных и других).
- фондов рискованного капитала, кредитных учреждений и банков;
- национальных, региональных и международных информационных центров, снабжающих всех участников купли-продажи конкретного вида технологии информацией, в том числе и о зарубежных рынках;
- региональных и национальных союзов и консорциумов, холдингов и т. д., содействующих развитию рынков конкретных видов технологии.

7.1.3. Виды коммерческих международных операций

[^]

Объектами международных коммерческих операций являются материально-вещественная продукция и услуги, включая результаты производственного и научно-технического сотрудничества, приобретающие в обмене форму товара. Эти объекты определяют виды коммерческих операций, осуществляемых на мировом рынке.

Международные коммерческие операции подразделяются на основные, осуществляемые на безвозмездной основе между непосредственными участниками этих операций (контрагентами разных стран), и обеспечивающие, связанные с продвижением товара от продавца к покупателю.

К основным коммерческим операциям относятся операции:

- по обмену научно-техническими знаниями (в форме торговли патентами, лицензиями, «ноу-хау»);
- по обмену техническими услугами (консультативный и строительный инжиниринг);
- технологический обмен;
- по предоставлению консультационных услуг в области информации и совершенствования управления.

Осуществление международных операций требует применения определенных правовых форм и использования конкретных методов их проведения.

Правовой формой, опосредствующей международные коммерческие операции является международная торговая сделка, обязательное условие которой — заключение ее иностранным контрагентом.

Под международной торговой сделкой понимается договор (соглашение) между двумя или несколькими сторонами, находящимися в разных странах по поставке установленного количества товарных единиц и/или оказания услуг в соответствии с согласованными сторонами условиями.

Международный характер договора вытекает из того, что его субъектами (сторонами) являются коммерческие предприятия (фирмы), находящиеся в разных странах. Договор купли-продажи не будет считаться международным, если он заключен между сторонами разной государственной (национальной) принадлежности, коммерческие предприятия (фирмы) которых находятся на территории одного государства (например, между филиалами и дочерними компаниями фирм разных стран, находящихся на

территории одной страны). В то же время договор признается международным, если он заключен между сторонами одной государственной (национальной) принадлежности, коммерческие предприятия которой находятся на территории разных государств.

Такое толкование договора содержится в конвенции ООН о договорах международной купли-продажи товаров (Венская конвенция 1980 года) и в Новой гаагской Конвенции о праве, применимом к договорам международной купли-продажи 1985 года.

Основные виды международных коммерческих операций можно охарактеризовать кратко следующим образом.

Операции по торговле научно-техническими знаниями (опытом) отличаются от операций по торговле материальными ценностями тем, что предметом международного обмена в них выступают результаты деятельности, которые принято считать «невидимым» товаром.

Операции по торговле научно-техническими знаниями связаны с обменом результатами производственных научных исследований и разработок, имеющих не только научную, но и коммерческую ценность. В качестве товара здесь выступают продукты интеллектуального труда, облеченные в форму патентов, лицензий, товарных знаков, промышленных образцов, представляющих собой часть так называемой промышленной собственности, а также технические знания и опыт, объединяемые понятием «ноу-хау», включающих передачу знаний и опыта путем предоставления технической документации, чертежей, секретов производства, не подлежащих патентованию.

Научно-технические знания поступают в международный оборот либо на основе купли-продажи (при продаже патентов), либо — отношений, возникающих в связи с получением временного права пользования результатами на базе международных лицензионных соглашений.

Операции по обмену лицензиями состоят в предоставлении права (разрешения) одной стороной — патентовладельцем, именуемым лицензором, другой стороне — лицу (или фирме), именуемому лицензиатом, на промышленное и коммерческое изобретения, пользующегося патентной защитой в течение обусловленного *срока* за определенное вознаграждение.

Предоставление иностранному контрагенту лицензий на использование изобретений, технических знаний и опыта, а также товарных знаков называется заграничным лицензированием.

Операции по торговле техническими услугами, получившими в международной практике название инжиниринговых. Как самостоятельный вид международных коммерческих операций инжиниринг предполагает предоставление на основе договора на инжиниринг одной стороной, именуемой консультантом, другой стороне, именуемой заказчиком, комплекса или отдельных видов инженерно-технических услуг, связанных с проектированием, строительством и вводом объекта в эксплуатацию; с разработкой новых технологических процессов на предприятия заказчика; усовершенствованием имеющихся производственных процессов вплоть до внедрения изделия в производство.

Предоставление на основе договора на инжиниринг полного комплекса услуг и поставок, необходимых для строительства нового объекта, называется комплексным инжинирингом. Он включает три отдельных вида инженерно-технических услуг, каждый из которых может быть предметом самостоятельного договора:

- консультативный инжиниринг, связанный главным образом с интеллектуальными услугами в целях проектирования объектов, разработки и планов строительства и контроля за проведением работ;
- технологический инжиниринг, состоящий в предоставлении заказчику технологии или технологий, необходимых для строительства промышленного объекта и его эксплуатации (договоры на передачу производственного опыта и знаний), разработки и планов строительства и контроля за проведением работ;
- строительный и/или общий инжиниринг, состоящий главным образом в поставках оборудования, техники и/или монтажа установок, включая в случае необходимости инженерные работы. Инженерно-консультационные услуги предоставляются в виде технической документации, результатов исследований, исходных данных для строительства, экономических расчетов, смет, рекомендаций и т. д.

В этой работе следует руководствоваться разработанным (в 1982 г.) группой экспертов по международным договорам на поставку промышленной продукции Комитета по развитию торговли ЕЭК ООН «Руководством по составлению международных договоров на консультативный инжиниринг, включая связанные с этим аспекты технического содействия». Оно

содержит подробный перечень и характеристику условий, необходимых для включения в договор между консультантом и заказчиком, а также перечень услуг, предоставляемых инженером-консультантом. В него включаются, в частности, следующие услуги:

- проведение предварительных технико-экономических обоснований и исследований, связанных с общим проектированием;
- планирование и подготовка чертежей и смет расходов;
- подготовка предварительных эскизов, проектной документации, детальных чертежей и спецификаций;
- планирование и составление программы финансирования;
- подготовка технических условий для участия в торгах и выдача рекомендаций по поступающим предложениям;
- оценка предложений о строительстве объектов;
- контроль за строительством, изготовлением оборудования, монтажом, наладкой и пуском оборудования в эксплуатацию;
- выдача сертификатов о качестве проведенных работ и других.

Сотрудничество по реализации коммерческих операций международного производственного и научно-технического сотрудничества зарубежных фирм выступает как результат определенной организационно-управленческой деятельности, целью которой является заключение соглашений:

- о специализации и кооперировании производства;
- об организации совместного строительства объектов и их эксплуатации;
- о поставке крупных промышленных объектов с компенсацией (оплатой) товарной продукции;
- о кооперации в области научных исследований и других.

Реализация этих соглашений осуществляется на основе заключения международных коммерческих сделок. Поэтому область производственного и научно-технического сотрудничества входит в сферу международной торговли.

Из анализа совместной деятельности с зарубежными представителями, очевидно то, что любые соглашения между двумя фирмами (компаниями) заключаются при непосредственном контакте, т. е. на официальных встречах, переговорах.

Любая договоренность о сотрудничестве оформляется

соответствующими договорами.

Хотя одним из наиболее важных условий, используемых в международной практике, при заключении подобного рода договоров является условие об обеспечении защищенности информации в отношении предмета договора, без включения такого условия нельзя сохранить существенный элемент сделки — конфиденциальность.

Такое условие должно включать в себя следующее:

1. взаимное обязательство сторон принимать все необходимые меры для предотвращения разглашения коммерческой тайны с перечислением основных мер;
2. документы или изделия, указанные в договоре, будут рассматриваться сторонами как строго конфиденциальные;
3. стороны берут на себя обязательства принимать все необходимые меры для предотвращения нарушений правил пользования этими документами или изделиями, установленных в соответствующих статьях договора;
4. стороны обязуются не передавать без предварительного согласия другой стороны оригиналы документов или изделий, их копии или репродукции любого рода третьим сторонам;
5. стороны обязуются обеспечить ознакомление с информацией, составляющей коммерческую тайну предмета договора, только лишь строго ограниченного числа своих работников, с которых должны быть взяты подписки о неразглашении информации, составляющей коммерческую тайну, содержащейся в предмете договора или являющейся предметом договора.

Нарушение такого рода требований договоров может привести к его аннулированию и привлечению виновников к ответственности в соответствии с действующим законодательством.

7.1.4. Научно-техническая документация - источник конфиденциальной информации [^]

В состав научно-технической документации входят:

- научно-исследовательская (научная), конструкторская, технологическая, проектная и другая производственная документация;

■ кино-фотодокументы, документы на машиночитаемых носителях:

—документы по изобретениям и открытиям;

— геолого-геодезические, метеорологические, экологические и другие документы.

Научно-технические документы в зависимости от способа их выполнения и характера использования подразделяются на оригиналы, подлинники, дубликаты, копии и эскизы.

Виды научно-технических документов

1. Научно-исследовательская (научная) документация:
 - a. итоговые и этапные отчеты о НИР и ОКР;
 - b. технические отчеты;
 - c. заключения, отзывы и рецензии;
 - d. аннотации, паспорта, регламенты;
 - e. монографии, диссертации и отзывы на них;
 - f. рукописи неопубликованных научных работ;
 - g. рекомендации различного характера;
 - h. технические задания на НИР, ОКР;
 - i. программы НИР;
 - j. технико-экономические обоснования, обзоры, доклады;
 - k. первичная документация в процессе НИР, ОКР, ОТР и ЭПР (ОТР — опытно-технологическая, ЭПР — экспертно-проектная): журналы записей, экспериментов, различных анализов; дневники; кино-фотодокументы; документы на машинных носителях.
2. Конструкторская документация (КД) — это совокупность графических и текстовых конструкторских документов, которые самостоятельно или в совокупности определяют состав и устройство изделия и содержат необходимые данные для его разработки или изготовления, контроля, приема эксплуатации и ремонта. Включает:
 - a. технические предложения;
 - b. эскизные проекты;
 - c. технические проекты;
 - d. рабочую конструкторскую документацию.
3. Технологическая документация (ТД) — это сово-

купность графических и текстовых технологических документов, которые самостоятельно или в совокупности определяют технологический процесс изготовления изделий промышленного производства или процесс сооружения объектов капитального строительства.

4. Проектная документация (ПД) — это совокупность технических документов, фиксирующих процесс и результаты проектирования.
5. Документы автоматизированных систем обработки данных и автоматизированных систем проектирования.

Критерии ценности НЦ

На каждом этапе экспертизы ценности НТД применяется в комплексе система общих и специфических критериев.

К общим относятся критерии:

- происхождение: организация, роль и место организации в системе организаций страны или в конкретной отрасли; значимость выполняемых ею функций; время и место создания; авторство документов.
- содержание: значимость проблемы и объекта, отраженного в документах; значение содержащейся в документах информации, ее повторение в других документах; целевое назначение, вид и разновидность документа.
- внешние особенности: юридическая содержательность документа — наличие подписей, дат, печатей; наличие резолюций, помет; особенности передачи документа, текста, подлинность; особенности материальной основы документа; особенности физического состояния, полноты, сохранности документа.

К специфическим относятся критерии:

- принципиальная новизна, уникальность, оригинальность решения проблемы, конструкции, технологии, проекта;
- степень отражения уровня науки и техники, производства на данном этапе развития общества;
- значимость проблемы, проекта, модели, конструкции, технологии на момент внедрения для развития конкретных отраслей производственной и хозяйственной деятельности;
- экономическая эффективность внедрения результатов исследования или технической идеи;

- социальная эффективность исследования или разработки.

7.1.5. Возможные условия разглашения сведений, составляющих коммерческую тайну [^]

По мере развития рыночных отношений и расширения внешнеэкономических связей российских фирм у иностранных партнеров и конкурентов все чаще появляются устремления к сведениям о планах фирмы, ее финансовом положении, методах управления, рыночной стратегии.

Возникновение конкуренции также порождает между ними подобные устремления.

Построение системы защиты коммерческой тайны фирмы более чем необходимо при регулярном сотрудничестве с иностранными представителями. Построение такой защиты целесообразно начать с определения открытых источников и соответствующих им возможных официальных каналов распространения конфиденциальной информации.

С учетом специфики научно-технической и коммерческой деятельности, степенью развития связей с деловыми партнерами хотелось бы выделить перечень официальных каналов передачи информации при таком взаимодействии:

- выступления сотрудников фирмы с докладами и в дискуссиях на международных конференциях и симпозиумах, проводимых в России и за рубежом;
- передача информации в процессе общения с иностранными журналистами;
- демонстрация научно-технических фильмов;
- демонстрация действующих объектов научно-технических достижений (оборудования, изделий, технологии);
- демонстрация научно-технических достижений на выставках, проводимых в России и за рубежом;
- все виды рекламы экспортной продукции в форме печатных изданий — брошюр, стендовой литературы для выставок и ярмарок;
- обмен с зарубежными научными учреждениями, предприятиями и фирмами отчетами о НИОКР в соответствии с соглашениями о научно-техническом сотрудничестве или о совместном выполнении

исследования и разработок;

- публикация научных, технических и других материалов в зарубежных и международных изданиях;
- передача информации при переписке с зарубежными научными учреждениями и специалистами;
- передача сведений представителям иностранных фирм в процессе переговоров или при заключении экспертных или импортных соглашений;
- прием иностранных специалистов на территории фирмы;
- проведение совместных разработок (проектов, экспериментов) в рамках осуществления научно-технических связей.

Каждый из вышеуказанных каналов характеризуется весьма значительными объемами передачи информации зарубежными партнерами.

Анализ, поступающих по открытым каналам сведений позволяет иностранным экспертам получать сообщения о деятельности фирмы, ее достижениях и другую ценную информацию.

Для сбора интересующей информации зарубежные фирмы активно используют различные приемы добывания информации особенно на международных выставках. Путем опроса и анкетированная российских специалистов получают подробную информацию об их месте работы, тематике проводимых ими исследований и разработок.

Основным «производителем» и «держателем» информации является человек. Это первичный канал как возникновения, так и утраты любого объекта интеллектуальной собственности. Исходя из этого основное внимание должно быть уделено сотрудникам фирмы, начиная от момента их поступления на работу.

Миграция специалистов, особенно имевших дело с конфиденциальной информацией, — самый основной и трудно контролируемый канал утечки информации. Так, получившая у нас в последнее время широкое распространение практика разного рода совместительства сотрудников, прежде всего научно-исследовательских организаций, где они используют свои профессиональные знания, опыт и навыки, приобретенные по основному месту работы, т. е. фактически интеллектуальный продукт организации, только должным образом не оформленный в ее собственность, является одним из наиболее вероятным каналом утечки информации. По опыту зарубежных стран и после увольне-

ния сотрудника (по крайней мере, в течение года) внимание к его дальнейшей деятельности не должно ослабевать.

Особыми каналами утраты интеллектуальной собственности или, по крайней мере, ее коммерческой ценности являются совместные работы с другими фирмами, контакты с клиентами и инвесторами, где особое место занимают переговоры. (Так, например, в *целях* сбора интересующей их информации инофирмы нередко идут на создание совместных предприятий.)

Не следует упускать из виду также технические средства недобросовестной конкуренции (промышленного шпионажа), которые все чаще проникают и на наш внутренний рынок. Тем более, что многие производственные процессы сопровождаются явлениями, имеющими физическую, химическую, биологическую и иную природу, в результате которых переносится та или другая информация.

Анализ и обобщение возможных путей утраты интеллектуальной собственности (следовательно, и мероприятий по их перекрытию) должны вестись по следующим основным направлениям:

1. Люди.
2. Документы.
3. Изделия — процессы.

Учитывая большое количество и разнообразие конкретных каналов утечки информации, наиболее целесообразным является построение работы именно исходя из перечисленных направлений. Разработку мероприятий по сохранению коммерческой тайны предприятия следует осуществлять, соблюдая принцип комплексного перекрытия возможных каналов утечки информации и обеспечения равнозначной надежности защиты всех ее носителей.

Защита от утечки конфиденциальной информации полностью ложится на саму фирму. Необходимо самим постоянно проявлять заботу о защите собственных передовых технологий, новых научных идей и результатов перспективных разработок. Целесообразно задерживать публикации о полученных научных результатах, выхолащивать из них сведения, представляющие интерес для научной общественности, ограничивать доступ к ней широкого круга лиц.

В процессе проведения совместных встреч, где обстановка общения, характеризующаяся сравнительно большим количеством участников, присутствием посторонних лиц, необходимо

придать огласке конфиденциальную информацию, сложностью контроля за поведением участников и т. п., объективно создают условия повышенной уязвимости информации.

Следовательно, все это ставит организацию перед необходимостью принятия мер по защите собственных информационных ресурсов, в процессе реализации которых решаются задачи в совокупности по следующим направлениям:

- отбор и группировка информации, подлежащей оглашению;
- разработка и реализация правил проведения со звещаний и переговоров, приема посетителей;
- организация работы с персоналом, т. е. лицами, которым поручена организация и проведение со звещаний и переговоров, ответственными за прием посетителей;
- проведение мероприятий по обеспечению требований, предъявляемых к помещениям, где проводятся совещания и переговоры; их охрана.

7.1.6. Экспертиза ценности передаваемой научно-технической документации [^]

Экспертиза ценности конструкторской документации

Экспертизе подвергаются:

- на стадии «эскизный проект» — ведомости эскизного проекта и пояснительные записки;
- на стадии «технический проект» — чертежи общих видов изделий; ведомости технического проекта; пояснительные записки; патентный формуляр; карты технического уровня и качества продукции; технико-экономические показатели;
- на стадии «рабочая документация» — сборные чертежи изделия; габаритные и монтажные чертежи, схемы, технические условия, расчеты экономической эффективности изделия, спецификации, акты (государственных, отраслевых, фирменных) испытаний и приемки изделия, групповые конструкторские чертежи; кино-фотодокументы, отражающие процесс обработки, изготовления и испытания изделия; спецификации по видам обеспечения; инструкции по ведению массивов данных в АС ОД и САПР; каталоги баз данных, тексты

программ, описания языков; положения о службе САПР и другие.

Экспертиза ценности технологической документации

Экспертизе подвергаются:

- технологические документы, отражающие новые технологические процессы, методы организации производства и труда, экономии материалов;
- чертежи универсального технологического оснащения для механической обработки деталей, сборки изделий, которые могут применяться для нескольких изделий, цехов, предприятий;
- документация по технологической оснастке, отличающаяся новизной и совершенством конструкции;
- технические документы на приспособления для совершенствования технологических процессов.

Особое внимание уделяется экспертизе таких документов как:

- маршрутные карты, технологические инструкции, правила, рецептура, описания, диаграммы, характеристики, схемы, режимы производства, ведомости технологической оснастки, карты основных и типовых технологических процессов, карты уровня аттестуемой продукции, регламенты;
- технические условия на изготовление изделий основного производства, альбомы технологических процессов, чертежей измерительных и контрольных приборов и инструментов;
- технико-экономические показатели, нормы расходов материалов, технологические паспорта, спецификация основного технологического оборудования.

Экспертиза ценности приемной документации

Экспертизе подвергаются:

- задания на проектирование продукции, проекты размещения строительства, проекты планировки, отчеты об изысканиях, генеральный план, ситуационный план, общая (сводная) пояснительная записка, схемы и

описания технологических процессов и оборудования, основные чертежи архитектурно-строительной части, чертежи цехов, фотографии общего вида зданий, корпусов и цехов, чертежи уникального характера; планы расположения зданий, транспортных путей, подземных сетей и ограждений; планы размещения оборудования, генеральные сметы к проектам реконструкции, сметно-финансовые расчеты.

7.2. Организация работы с зарубежными партнерами [^]

7.2.1. Оценка потенциальных партнеров [^]

Важную роль для предприятия играет выбор партнеров по совместной деятельности, так как от сделанного выбора во многом зависит успех задуманного предприятия или сделки. При выборе партнера для совместной деятельности приходится сталкиваться с тем, что в России до сих пор не существует стройной информационной системы для получения сведений об организациях и фирмах-участниках рынка, поэтому российским предприятиям пока приходится полагаться на удачу и на свои силы.

Успешный выбор надежного партнера можно осуществить только освоив и адаптировав для наших условий систему поиска партнеров, действующую на Западе, где, чтобы свести к минимуму коммерческие риски, выработана система банковских гарантий, страхования контрактов и другие механизмы, незнание или неприменение которых приводит к значительным убыткам.

Деловые качества возможной фирмы-партнера должны оцениваться с правовой, коммерческой, финансовой и технической точек зрения. Для получения этих данных следует пользоваться следующими документами:

1. Нотариально заверенными копиями учредительных документов: договора и уставы, которые дадут сведения о правовом статусе фирмы, размере капитала и профиле ее деятельности.
2. Проспектами и каталогами, публикуемыми самой фирмой, в которых также содержатся основные данные

о ней, а так же о наличии отделений и филиалов, сбытовой сети и клиентуре.

3. Балансами доходов, расходов и отчетов (тоже публикуемыми фирмой), которые дадут представление о состоянии кредиторской и дебиторской задолженности, объемах распродаж, акционерном капитале и акционерах, размере начисленных дивидендов.
4. Справочниками различных видов. Технические и коммерческие справочники, содержащие общие сведения о производственной и коммерческой деятельности фирмы, ее отделений и филиалов в России и за рубежом с указанием адресов и телефонов. Справочники бывают как общего характера, так и по отраслям производства, по акционерным обществам, а также международные и национальные. Для изучения связей между фирмами очень важна информация, содержащаяся в справочниках руководящего состава фирм. В них присутствуют списки директоров и занимаемых ими в различных обществах постов. А в специальных справочниках публикуются биографии людей делового мира. Всю информацию по нужным справочникам можно получить в торговых палатах соответствующих стран.

Во избежание всякого рода конфликтов исключительно важное значение могут иметь личные качества будущего партнера. Конфиденциальную информацию о личности интересующего вас бизнесмена можно получить, обратившись в кредитные конторы или бюро, которую те, в свою очередь, добывают через сеть своих агентов. Пользуясь ими, следует иметь в виду, что за достоверность информации конторы и бюро никакой ответственности не несут.

О платежеспособности фирмы более надежны данные коммерческих банков, так как им известно финансовое положение фирм в течение длительного времени. Они в состоянии даже предвидеть рост их доходов или банкротство, потому что изучают и знают все стороны коммерческой деятельности своих клиентов.

Важные сведения о фирме можно почерпнуть из публикаций в прессе: данные местных торговых палат, различных ассоциаций или иных объединений промышленников, следящих за коммерческим престижем и деловой репутацией своих членов, мнения конкурентов. Немало информации можно почерпнуть из газеты «Коммерсант», в которой регулярно печатаются данные об

учредителях, их адреса и телефоны. В официальных публикациях содержатся решения о примененных санкциях к фирмам, нарушившим экспортные или импортные запреты. Например, в США сведения о лишении экспортеров экспортных привилегий на определенный срок и иных санкциях за нарушение экспортного контроля публикуются в «Федеральном реестре». Такие сведения характеризуют фирму, попавшую в «черный список» с негативной стороны.

Кроме всего сказанного, хорошо бы еще выяснить, не допускала ли интересующая вас фирма каких-либо акций, направленных на дискредитацию будущих партнеров, взаимоотношения ее с конкурентами на внутреннем и внешних рынках.

Сведения о фирме можно получить и в государственных или иных организациях, содействующих внешнеэкономическим связям: торговых палатах, министерствах торговли, в консульских учреждениях, различных национальных государственных ведомствах и центрах, ведающих вопросами внешней торговли, а также в различных частных федерациях, ассоциациях торговых и промышленных фирм, институтах, информационных центрах и выставках.

В таких отчетах обычно содержится полное название фирмы, дата и номер регистрации, начальный капитал, состав правления и акционеров, представительские полномочия, сфера деятельности, номенклатура экспорта и импорта, численность персонала. В финансовых разделах приводится динамика оборота, движение средств по счетам, называются банки, чьими клиентами является фирма. Кратко характеризуется выполнение платежных обязательств.

Пользуясь этими источниками информации, надо учитывать, что сведения, получаемые из фирменных справочников, проспектов, каталогов и рекламы, а также кредитных и справочных бюро не являются вполне объективными, поскольку их материалы основываются на данных самих фирм и характеризуют их только в положительном свете. Поэтому мнение об интересующей фирме можно составить только после изучения всех названных источников информации. При этом надо учитывать, что информация о фирме, основанная на личных контактах, может оказаться более надежной, чем красочные и внешне эффектные проспекты и каталоги.

Для сбора и накопления информации о фирмах, с которыми

планируется сотрудничество и уже ведется работа, хотелось бы предложить вариант Информационной накопительной карты, в которую постоянно заносятся данные о фирмах «конкурентах».

Таким образом, своя накопительная информация, должна сыграть положительную роль при выборе партнера и при дальнейшем взаимодействии с ним. При выборе зарубежных партнеров необходимо учесть следующие моменты:

При заключении внешнеэкономической сделки необходимо отдавать предпочтение тем фирмам, которые предложат лучшие условия (по качеству, срокам, кредитам, ценам), касается ли она экспорта или импорта, является ли компенсационной или бартерной, идет ли речь о разовой сделке (мелкой или крупной) или о долгосрочных отношениях, осуществляется ли купля-продажа товара, лизинг.

Но если речь идет о сотрудничестве на долгосрочной основе, подход должен быть иным. С особой тщательностью нужно проверять надежность зарубежного партнера. Желательно, чтобы партнером была крупная фирма, зарекомендовавшая себя на мировом рынке со всех сторон.

Подобные сведения о фирмах должны быть всегда под рукой. В этой связи необходимо иметь свою базу данных различных зарубежных представительств.

7.2.2. Прием иностранных представителей и проведение коммерческих переговоров [^]

Деловые совещания и переговоры являются разновидностями делового общения, формами обмена информацией в деловой сфере.

С расширением круга предпринимателей России, активно действующих на внешних рынках, существенно возрастает роль переговоров с иностранными партнерами. Многие вопросы требуют прямого обсуждения: условия сделок, порядок поставки товаров, транспортировки грузов, проблемы страхования и т. д. Не секрет, что успех переговоров зависит от прочности позиций участников, конъюнктуры рынка, конкретных интересов партнеров. При этом немаловажную роль играют и такие факторы, как умение вести торг, психологические особенности партнеров и другие слагаемые, в совокупности образующие «искусство переговоров». Овладение им требует определенных навыков, соблюдения общепризнанных норм.

Планирование переговоров

Планирование переговоров позволяет найти и устранить возможные подводные камни, заранее предусмотреть, какие неожиданные проблемы могут возникнуть в ходе переговоров, своевременно продумать необходимые действия и мероприятия, а также вовлечь в подготовку к переговорам нужных работников. Важно продумать использование вспомогательных средств — диаграмм, таблиц, слайдов, видеофильмов и т. п.

Обычно переговоры состоят из следующих этапов:

- начало беседы;
- передача информации;
- выдвижение аргументов;
- комментарии (в случае необходимости — опровержения) к доводам партнера по переговорам;
- согласование взаимоприемлемых решений;
- подведение итогов переговоров и принятие решений.

Данная последовательность может быть изменена в зависимости от обстоятельств. Наиболее важен завершающий этап.

На характер переговоров влияет следующее:

- профессиональный опыт и знания;
- ясность, четкость, доступность, наглядность изложения;
- постоянная нацеленность на достижение нужных результатов;
- умение варьировать интенсивностью переговоров;
- необходимость соблюдать разумные пределы при передаче информации;
- способность поддержать доверительность в переговорах;
- умение варьировать выдвигаемые аргументы;
- умение использовать различные эмоционально выразительные средства, усиливающие воздействие на собеседника.

В начале беседы важно создать непринужденную атмосферу, интерес к обсуждаемому вопросу.

Психологически основная задача первых моментов переговоров — попытаться воздействовать на партнера таким образом, чтобы снять у него напряженность. Первые две-три фразы должны создать у партнера положительную расположенность. Исключить попытки загнать партнера в угол, принудить его к оборонительной позиции. Нельзя не считаться с возрастом собеседника, его национальными особенностями, личными

пристрастиями (если что-либо о них известно). Вполне уместны комплимент, несколько теплых слов, шутка, дружеская тональность в разговоре. После этого можно перейти к изложению сути дела.

Необходимо избегать таких оборотов, как «Я бы предложил»; «Я бы хотел» и т. д. Лучше употреблять фразы типа: «Как Вы относитесь к такому предложению, как...»; «Вы, вероятно, заинтересуетесь, узнав, что...» и т. п.

Дать почувствовать партнеру, что его ценят как личность, профессионала, специалиста.

Вилы переговоров

Существуют различные классификации видов переговоров. Наиболее традиционная — по их содержанию и целям.

1. Переговоры по установлению новых отношений и обязательств между партнерами.
2. Переговоры по развитию ранее достигнутых договоренностей.
3. Переговоры с целью урегулирования конфликтной ситуации.
4. Переговоры по изменению сложившихся договоренностей в свою пользу.
5. Переговоры по достижению определенных побочных результатов, нашедших отражение в ранее принятых договоренностях.

В зависимости от ситуаций, в каких они проводятся, различают переговоры по урегулированию кризисных или конфликтных ситуаций и переговоры, ведущиеся в рамках нормального делового сотрудничества. В первом случае к переговорам нередко привлекаются посредники, возникает необходимость неофициальных контактов

Переговоры могут быть двусторонними и многосторонними, что обуславливает определенный характер их ведения.

Подготовка и ведение переговоров

Как правило, задолго до того как партнеры сядут за стол и начнут непосредственно обсуждать вопросы, составляется план ведения переговоров. Примерная схема подготовки такова:

- анализ сложившейся ситуации участников, повестки дня;
- инициатива проведения переговоров и определение

- предстоящих к обсуждению задач;
- выработка стратегии и тактики переговоров;
 - разработка подробного плана подготовки к переговорам;
 - сбор информации и материалов; классификация информации в зависимости от целей каждого этапа переговоров;
 - систематизация и отбор информации;
 - составление рабочего плана переговоров;
 - проведение подготовительных рабочих совещаний участников предстоящих переговоров;
 - разработка концепции переговоров, ее письменное изложение.

Готовясь к переговорам, необходимо обдумать собственные цели, определить темы, которые могут быть затронуты в их процессе, наметить возможных участников.

Инициатива в переговорах зависит от интуиции, активности и возможности своевременно провести предварительный анализ. Это позволяет контролировать ситуацию. Ни в коем случае нельзя терять инициативу как на этапе подготовки переговоров, так и в ходе их проведения.

Подробный план переговоров предусматривает четкую программу действий: устанавливаются объем и виды потребной информации, определяются примерные затраты на подготовку, выделяются соответствующие работники, перед ними ставятся конкретные цели.

Наиболее сложным и трудоемким процессом является сбор информации. Например, готовясь к первой встрече с представителем иностранной фирмы, необходимо как можно больше узнать о ее достижениях, «теневых» местах. В случае недостатка информации можно обратиться к соответствующим консультационным фирмам как в России, так и за рубежом. В необходимых случаях — в Министерство внешних экономических связей.

Объем потребной информации зависит от общей эрудиции, уровня профессиональных знаний и личной мотивации сотрудников фирмы, которым предстоит вести переговоры. Продолжением работы с информацией является ее сбор и систематизация. Необходимо освободиться от второстепенных сведений, сгруппировать полученные данные соответственно задачам переговоров. Важно определить характер и объем информации, которую необходимо передать партнеру по переговорам,

предварительно взвесив, как эта информация будет им интерпретирована.

При переговорах одним из основных являются ценовые вопросы. Заблаговременно информационный отдел должен собрать всю доступную информацию по ценам мирового рынка. Если в переговорах затрагивается возможность экспорта продукции, необходимо сосредоточить сведения, выгодно раскрывающие преимущества выпускаемого товара (технические характеристики, потребительские свойства и т. д.). К этому моменту желательно иметь условия конкурсов, сведения о которых всегда должны быть под рукой.

Интересующая информация должна быть оценена с точки зрения достоверности и надежности ее источников.

В переговорах по импорту также требуется знание цен, условий поставки, состояния конъюнктуры рынка и сложившихся традиций.

Вступая в переговоры с фирмой, нужно располагать максимумом данных о ней, степени ее надежности. Досье о партнере включает характер деятельности фирмы, ее юридическую форму и форму собственности, виды производимой продукции (профиль товаров, торговые операции), финансовое состояние фирмы, ее ценовую и финансовую политику, заинтересованность в деловых контактах. Необходимо знать связи фирмы с конкурентами и условия, на которых она ведет сделки с ними, навести справки об основных финансово-экономических показателях (размеры акционерного и собственного капитала, оборот, активы, прибыль, число собственных сотрудников), руководящем составе фирмы. Информационный отдел должен отследить статьи о партнере в газетах и журналах, иметь отзывы коллег.

Разрабатывая сценарий переговоров, необходимо попытаться увязать уже имеющуюся информацию с собственными представлениями в единое целое. Целесообразно продумать психологические аспекты предстоящих переговоров, их начало и завершение, как бы мысленно прорепетировать свои соображения, которые можно высказать партнеру, чтобы добиться желаемого результата.

При планировании переговоров следует учитывать возможность появления непредвиденных обстоятельств и отрабатывать навыки гибкой реакции на неожиданные повороты, которые могут возникнуть по инициативе партнера.

Планирование переговоров включает следующие моменты:

- разработка прогноза переговоров;
- определение установок на переговоры, выделение основных задач;
- поиск оптимальных средств решения стратегических задач переговоров;
- разработка «дерева целей» — как долгосрочных, так и краткосрочных — на весь процесс переговоров, определение их взаимосвязи и последовательности реализации;
- выработка средств реализации этих целей, своевременная подготовка к преодолению трудностей, возникающих в процессе подготовки к переговорам.

Техника веления переговоров

В соответствии с правилами приема делегаций, ответственные лица доставляют гостей за 5 — 7 минут до планируемого начала переговоров. Это позволяет членам делегации освоиться с обстановкой, подготовиться к встрече. Если переговоры ведутся не первым лицом фирмы, целесообразно отвести время на короткую встречу первого лица и делегации для обмена приветствиями.

Для ведения записей и обобщения результатов переговоров заранее выделяется соответствующий сотрудник. Если в них участвует переводчик, то необходимо создать ему благоприятные условия.

Как правило, переговоры ведут руководители делегаций. Нельзя перебивать их выступления, вносить уточнения, устраивать перекрестные мини-переговоры параллельно с выступлениями руководителей делегаций. Это нетактично и сильно мешает нормальному процессу переговоров.

До начала переговоров необходимо проинформировать членов своей делегации о фирме, с которой будут вестись переговоры. Информация формируется из различных источников — справочников, заказных работ специальных консультативных фирм (российских и зарубежных), запросов в российские коммерческие представительства.

На первой встрече прежде всего следует познакомиться иностранную делегацию с участниками переговоров со своей стороны, обменяться визитными карточками. Кроме этого, обычно

имеет место обмен общими фразами, а затем знакомство гостей с программой их пребывания в России ее уточнения, если будут замечания со стороны иностранных представителей.

Если встреча с представителями данной фирмы осуществляется впервые, целесообразно ознакомить гостей с характером деятельности своей организации, особенностями выпускаемой продукции, объемом производства и т. д., после чего попросить своего партнера рассказать о его организации.

Фирме имеющей производственный характер, целесообразно включить в программу пребывания делегации ознакомление со своей деятельностью. Необходимо подготовить персонал к такому визиту, заранее определить объем передаваемой информации.

Информация, поставляющая интерес при влени переговоров

Информационный отдел фирмы на основе аналитических исследований предварительно выявляет, какая информация в первую очередь интересует зарубежного предпринимателя:

1. Размер рынка.
2. Динамика изменения рынка.
3. Издержки по ведению дела.
4. Степень риска.

Основная часть интересующей иностранного предпринимателя информации, особенно касающейся размеров и динамики рынка, может быть им получена из открытых источников, статистических отчетов, средств массовой информации и т. д. Что же касается оценок издержек производства, конкурентных преимуществ и степени риска, то они не могут быть произведены с приемлемой достоверностью без информации, характеризующей вполне определенного потенциального партнера, т. е. какую-то конкретную фирму.

К такой информации в соответствии со сложившейся практикой можно отнести данные по следующим вопросам:

- предполагаемая экономия за счет дешевизны рабочей силы;
- величина транспортных расходов;
- потребности в сырье, материалах, комплектующих изделиях и обеспечение ими;
- состояние и стоимость основных и оборотных фондов;
- производственные мощности;

- организация производства;
- финансовое положение и т. д.

В последнее время отличается рост ценности информации о российских предприятиях и спрос на нее. Этот спрос неизбежно порождает соответствующее предложение. Причина появления этого предложения заключается в том, что иностранные фирмы не имеют, как правило, достаточной информации о российских предприятиях и фирмах, и их информационные запросы стимулируют появление различных посреднических организаций, специализирующихся на информационном обеспечении как российской, так и зарубежной клиентуры. Однако это не исключает возможность обращения некоторых инофирм к российским предприятиям напрямую. Поэтому, прежде чем давать о своей фирме хоть какую-нибудь информацию, необходимо убедиться в том, что представители иностранной компании пришли на переговоры не только с целью получения сведений о деятельности российской фирмы.

Сведения о российских и зарубежных фирмах можно получить в таких посреднических организациях, как: Российско-американский университет «Россия — США — бизнес — партнеры», центр научно-технического творчества «Акцепт», фирма «Снег» и другие. Занимаются такой же деятельностью некоторые российские предприятия: Министерство гражданской авиации, ленинградское ПО «Авангард» и т. д. Эти организации рассылают потенциальным клиентам анкеты, предложения, документы.

В этой практике нет ничего необычного, в международной предпринимательской деятельности такие способы получения необходимой информации имеют самое широкое распространение.

В обобщенном виде содержимое запрашиваемых сведений сводится, главным образом, к следующему:

1. Полное наименование предприятия, его место в структуре отрасли, почтовые реквизиты.
2. Данные о руководящем составе: фамилии, имена, отчества, номера служебных телефонов.
3. Профильные виды продукции, ее характеристики, сведения о направлениях научно-исследовательской деятельности.
4. Стоимость основных и оборотных фондов.
5. Финансовое положение.

- б. Планируемая к освоению продукция:
 - а. физические и стоимостные объемы;
 - б. то же, но с разбивкой для внутреннего рынка и экспорта.
7. Численность персонала и фонд заработной платы.
8. Потребности в сырье, материалах, комплектующих узлами деталях, источники удовлетворения этих потребностей.
9. Транспортные и энергетические потребности.

В конечном счете, в результате исследовательской деятельности у получателя информации могут накапливаться обширные материалы для сопоставления, обобщения и анализа. Следовательно, перед обладателем таких данных раскрываются возможности получения оценок по интересующим его направлениям деятельности предприятия (фирмы) или повысить точность и достоверность уже имеющихся у него сведений, а при благоприятных условиях — распространить полученные на основе этих сведений выводы на отрасль в целом.

При изучении иностранных источников и зарубежного опыта предпринимательской деятельности обращает на себя внимание тот факт, что на вопросы, подобные вопросам 5, 6, 7, 8, зарубежные фирмы, как правило, ответов не дают, т. к. указанные сведения составляют коммерческую тайну. В то же время наша хозяйственная практика знает примеры противоположного толка, когда предприятия (фирмы) легко расстаются со своими коммерческими секретами, никак не учитывая возможные экономические последствия этого.

Особенности переговоров при проложи «ноу-хау»

Особое место среди сведений, являющихся конфиденциальными, занимают «ноу-хау», под которыми понимаются конструктивные и технологические секреты, имеющие промышленную и коммерческую ценность и не защищенные патентным, международным и национальным законодательством.

При консультациях и ознакомлении с техникой и технологией зарубежные фирмы выработали способы ведения переговоров без раскрытия «ноу-хау».

Один из принципов защиты «ноу-хау» состоит в том, что любая информация о научно-технических достижениях, будь то

устная или печатная, должна носить сугубо рекламный характер. Если на переговорах потенциальный клиент настаивает на получении дополнительной информации о «ноу-хау», аргументируя это тем, что ему надо знать, за что он будет платить деньги, то используется специальная техника продажи «ноу-хау». Здесь необходимо обратить внимание на слова «потенциальный клиент», т. е. к этому времени необходимо иметь информацию об организации, с которой ведутся переговоры и лице, ее представляющем, что это — действительно потенциальный клиент.

Далее стороны заключают предварительное опционное соглашение, по которому потенциальный продавец обязан ознакомить потенциального покупателя с «ноу-хау», а последний, ознакомившись с ним, обязуется подписать лицензионное соглашение. В противном случае на основании опционного договора он не имеет права промышленно использовать «ноу-хау» и разглашать его, он теряет и определенную сумму денег, внесенную в депозит на счет продавца за ознакомление. Таким образом, вводится договорная охрана «ноу-хау».

Выводы

1. При попытках сторонних организаций установить с предприятием контакт следует прежде всего выяснить, в чем состоят их намерения, если это не вытекает из самого обращения к фирме. Кроме того, необходимо, используя имеющиеся возможности, навести справки об иностранной фирме, которая обратилась с запросом. Во многих случаях такая осведомленность о ней поможет избежать ошибок. Рекомендации по наведению таких справок описаны выше.
2. В случае, если обратившаяся иностранная компания заслуживает доверия, ее намерения соответствуют интересам фирмы и предполагается развивать намечающееся сотрудничество, необходимо выработать политику ведения переговоров. Не следует сразу же передавать все запрашиваемые сведения в полном объеме. Прежде всего необходимо убедиться в том, что запрашиваемые сведения соответствуют намерениям зарубежного потенциального партнера и действительно требуются ему для дальнейшего сотрудничества с фирмой. Особое внимание следует обратить на то, чтобы

- те сведения, которые решили представить зарубежной фирме, не раскрывали своих коммерческих секретов.
3. На стадии переговоров, когда суть взаимных намерений уже ясна, но юридически они еще не оформлены, было бы оптимальным ведение переговоров таким образом, чтобы ответы на вопросы зарубежного партнера носили индикативный характер, типа «да — нет», «можем — не можем» и т. п.
 4. После юридического оформления взаимных намерений можно оперировать более широкими данными об основных фондах, потребностях и другими сведениями, необходимыми для сотрудничества. При этом в рамках документа о намерениях или отдельным документом должны быть зафиксированы взаимные обязательства о неразглашении тех сведений, которые стороны определяют как конфиденциальные.
 5. Потенциальному партнеру следует раскрывать только те данные, которые относятся к сфере совместной деятельности.

Особенности передачи информации зарубежному партнеру

В данном случае под информацией подразумеваются сведения, соответствующие лучшему восприятию партнером точки зрения и помогающие уяснить его позицию.

При передаче информации следует внимательно следить за реакцией партнера. Этот процесс следует направлять таким образом, чтобы захватить инициативу в переговорах, побудить партнера сообщить нужную информацию, избегая при этом прямых вопросов.

Необходимо так задавать вопросы, чтобы на них нельзя было бы ответить только «да» или «нет», дабы не вызвать напряженности в беседе. Обычно такого рода вопросы задаются в тех случаях, когда необходимо получить согласие собеседника или подтверждение ранее имевшейся договоренности. Это предполагает осведомленность обоих партнеров по конкретному вопросу. Следует избегать опасности создания ситуации, когда у партнера может сложиться впечатление, будто ведется его допрос.

Другая категория вопросов — это так называемые открытые вопросы, требующие развернутого объяснения, например: «Как Вы относитесь к...»; «Каково Ваше мнение по вопросу о...»; «Почему

Вы считаете, что ...» и т. п. Они подразумевают последующий диалог на основе разъяснения точки зрения партнера, аргументированного изложения его позиции. В категорию открытых вопросов включаются «переломные», позволяющие получить информацию по наиболее уязвимым проблемам. Они задаются в тех случаях, когда уже имеется достаточно информации по данной проблеме и уже можно перейти к другой теме.

В тех случаях, когда необходимо добиться от партнера четких акцентов по той или иной проблеме, лучше задавать вопросы типа: «Правильно ли я понял, что ...»; «Считаете ли Вы, что...». Ответы на подобные вопросы создают благоприятную атмосферу для выработки единой точки зрения на обсуждаемый вопрос, а также для внесения поправок в позицию партнера.

В процессе обмена информацией облегчается переход к этапу аргументации, когда партнер более откровенно излагает собственную позицию, при этом может непроизвольно обнаружить свои слабые стороны.

С другой стороны, на этапе аргументации у партнера создается заинтересованность в поддержании переговоров.

Для успешного ведения переговоров важно умение внимательно слушать и правильно оценивать сказанное. В этом случае можно самому себе задать следующие вопросы:

- действительно ли я слушаю партнера или просто жду своей очереди высказаться?
- часто ли я отвлекаюсь?
- эмоционально ли реагирую на сказанное?
- часто ли перебиваю собеседника?
- не делаю ли поспешных выводов из сказанного?
- может быть, я не слушаю партнера, а просто обдумываю свой ответ?

Не следует забывать, что человек несведущий, мало знающий обычно многословен. И напротив, немногословный собеседник доказательнее обосновывает свою позицию. Зная это, нужно постараться избегать ненужной полемики, иначе может возникнуть угроза непреодолимой конфликтной ситуации.

Очень часто переговоры проигрывает тот, кто не умеет слушать другую сторону.

Вот некоторые условия, которые следует соблюдать:

- не отвлекаться на собственные мысли, сосредоточиться на теме беседы;
- слушая собеседника, не использовать это время на

подготовку собственных контраргументов.

При передаче партнеру информации:

- избегать начинать предложения с местоимения «я»;
- быть внимательным к собеседнику, когда он что-то говорит или спрашивает;
- следить за реакцией партнера, проявлением его эмоций;
- чаще обращаться к собеседнику по имени;
- следить за собственной речью, избегать неточностей, неясностей, при необходимости повторять особо важные положения;
- избегать монологов, стремиться к диалогу;
- не прерывать партнера;
- всем своим видом проявлять заинтересованность к тому, о чем говорит партнер;
- добиваться от партнера заинтересованности в получении информации;
- не употреблять двусмысленных выражений.

Переговоры — это поиск компромисса. Искусство достижения без излишней жесткости и неуступчивости. Вступая в переговоры, нужно видеть в партнере не противника, с которым будет жестокая схватка, а потенциального друга на долгое время. Необходимо рассчитывать на длительное сотрудничество.

В процессе беседы нередко возникает необходимость в чем-то убедить партнера. Это требует значительных усилий и сильных аргументов. Вместе с тем многое зависит от партнера, его способности, желания и готовности воспринимать аргументы.

Прежде чем излагать свои аргументы, необходимо убедиться:

- точна ли информация, на которой основываются аргументы?
- верны ли заключения?
- нет ли аргументации внутренних противоречий?
- можно ли привести подходящие примеры и сравнения?
- какие возражения и контрдоводы могут возникнуть у партнера?

Получая информацию от партнера, полезно убедиться:

- нет ли в аргументах партнера противоречий?

- можно ли оспорить приводимые факты и предположения?
- если в целом положение, выдвигаемое партнером, верно, не вызывают ли сомнение отдельные детали?
- не упрощает ли проблему партнер?
- правильно ли он оценивает доводы?

Чтобы доказательно обосновать свою позицию, полезно учитывать некоторые мелочи, которые могут оказаться решающими:

- необходимо оперировать простыми и убедительными доводами. Помнить, что партнер понимает из сказанного значительно меньше, чем он демонстрирует;
- небольшое число ярких аргументов достигает большего эффекта, нежели множество мелких и малоубедительных фактов;
- необходимо всегда открыто признавать правоту партнера, даже если это не вполне благоприятно;
- приспосабливаться к особенностям характера партнера, учитывать его опыт, знания, национальные особенности и т. п.;
- избегать простого перечисления фактов, опираясь на них, сформулировать выигрышные моменты своих предложений;
- оперировать понятиями, привычными для партнера.

Для того, чтобы тактически правильно построить аргументацию необходимо:

- излагать главные аргументы при любом удобном случае, но по возможности каждый раз несколько по-новому, соотносясь с конкретными обстоятельствами;
- в зависимости от психологических, национальных или иных особенностей партнера выбирать различные методы убеждения;
- избегать обострений, авторитарности в суждениях;
- предлагать партнеру варианты решения проблемы, чтобы вызвать или поддержать у него интерес к вашему предложению;
- персонифицировать аргументацию, убедительность

доказательств зависит прежде всего от их восприятия партнером, прежде постараться выявить его позицию, а затем использовать это при изложении своих доводов;

- чтобы добиться большей убедительности своих доводов, необходимо «подсказать» партнеру, какие выводы он может сделать, исходя из них;
- если партнер выдвигает контраргументы, на первый взгляд безупречные, нужно задуматься над тем, верны ли они, нет ли в них противоречий.

Завершение переговоров

Для данного этапа переговоров очень важен личный опыт, способность быть тактичным и внимательным к партнеру.

Основные задачи, решаемые на этом этапе сводятся к следующим:

- достижение основной или — в самом неблагоприятном случае — резервной, альтернативной цели;
- обеспечение благоприятной атмосферы в конце переговоров. Даже в случае, если главные цели переговоров не будут достигнуты, необходимо сохранить возможность поддержания дальнейших контактов;
- побуждение партнера к выполнению действий.

Совместное подведение итогов предполагает, что все участники переговоров имеют четкое и ясное представление по каждому пункту принятых решений и в соответствии с ними готовы начать реализацию плана конкретных действий.

Фаза окончания переговоров требует особого внимания, полной концентрации опыта, знаний и умений. Практика показывает, что лучше всего придерживаться правила — не спешить проявлять инициативу, но и не ждать слишком долго психологически удобного момента, иначе можно пропустить его.

Одним из признаков приближения окончания переговоров служит изменение поведения партнера — у него появляется расслабленность, усиливается или ослабляется эмоциональное восприятие слов, степень его участия в дискуссиях. Нужно быть готовым к тому, что партнер может принять неудовлетворительные решения. На этот случай должны быть подготовлены варианты, позволяющие продолжить переговоры и преодолеть

неблагоприятный настрой партнера.

Конечно, не все переговоры завершаются успешно. Такой исход обуславливается отсутствием со своей стороны убедительной аргументации или неготовностью партнера принять предлагаемое вами решение. Вполне логично и такое допущение, что другая сторона лучше подготовлена к переговорам, более опытна, чем вы. В процессе переговоров могут возникнуть препятствия, которые не зависят от обоих партнеров.

7.2.3. Порядок работы с зарубежными партнерами [^]

С целью установления единого порядка и режима работы с зарубежными партнерами, обеспечения защиты конфиденциальной информации разрабатывается «Инструкция о порядке работы с зарубежными партнерами», которой необходимо руководствоваться при контактах с представителями совместных предприятий и с представителями конкурирующих фирм.

Инструкция должна содержать следующие разделы:

- общие положения;
- основания для работы с зарубежными партнерами;
- формы работы с зарубежными партнерами (прием, организация деловых встреч, переговоров, посещение и прием зарубежных партнеров);
- организация работы по ведению телефонных разговоров, прием и отправка телексных сообщений;
- организация работы с документами, содержащими конфиденциальную информацию (обработка поступивших, изданных документов, ведение служебной переписки);
- организация работы при командировании за рубеж;
- оформление результатов работы с зарубежными партнерами, учет и отчетность.

Общие положения охватывают постановку проблемы защиты конфиденциальной информации при работе с зарубежными партнерами.

Основанием для контакта с иностранцами по служебной необходимости являются: планы международных научно-технических связей, заключенные контракты и протоколы, соглашения об установлении прямых производственных, научно-

технических связей, решения о совместной деятельности, а также инициатива самих зарубежных представителей и представителей российской стороны.

Прием зарубежных партнеров

Прием зарубежных делегаций осуществляется на основе утвержденных программ, составляемых по установленной форме, а также сметы расходов на прием.

Программы пребывания приглашенных иностранных делегаций и сметы расходов составляются отделом международных связей, которые затем утверждаются руководством фирмы за неделю до прибытия делегаций.

Ответственным за выполнение программы пребывания иностранной делегации является представитель соответствующего отдела.

Организация деловых встреч (переговоров)

Для участия в деловых встречах с иностранцами, как правило, должны привлекаться специалисты из числа сотрудников, выделенных для работы с иностранцами в количестве не менее двух человек. Переводчиков на деловые встречи приглашает отдел, принимающий иностранцев. Деловые встречи должны проводиться в специально выделенном помещении.

Оформление результатов работы с иностранцами

Отдел международных связей, принимающий иностранцев, по итогам работы с иностранными делегациями составляет отчеты произвольной формы. По итогам деловых встреч составляются записи бесед по установленной форме. Записи бесед представляются руководству в двухдневный срок после окончания работы с иностранцами, а отчеты, как правило, в двухнедельный срок (два печатных экземпляра).

В записях бесед и отчетах указывается: когда, где, с кем состоялась встреча, ее основание и цель; кем дано разрешение на встречу; какое учреждение, организацию или фирму представляли иностранцы; их фамилии и должностное положение; кто присутствовал со стороны фирмы; содержание беседы (существо вопросов и ответы на них); какая документация и какие образцы

изделий и материалов переданы иностранцам или получены от них, обязательства сторон по существу обсуждавшихся вопросов, а также другая заслуживающая внимания информация.

Отдел документационного обеспечения ведет учет деловых встреч, а также учет сообщений о контактах с зарубежными представительствами.

Организационные мероприятия

На этом этапе осуществляются организационные мероприятия по результатам работы с зарубежными партнерами.

Вся документация — отчеты по результатам работы с иностранными делегациями и записи бесед, содержащие обязательства и предложения сторон, докладываются отделом международных связей и отделом, организовавшим встречу, руководству фирмы.

Вся входящая иностранная корреспонденция, вне зависимости от ее вида, направляется в отдел документационного обеспечения для регистрации и первичного рассмотрения.

Входящая корреспонденция представляется руководству или направляется на рассмотрение и исполнение непосредственно в отделы. После рассмотрения руководством корреспонденция в соответствии с резолюцией направляется исполнителям, и контроль за сроками исполнения поручений осуществляется в соответствии с установленным порядком. Право подписи корреспонденции в адрес иностранцев имеют руководитель, его заместители, начальники отделов и их заместители (по отдельным вопросам).

Любая корреспонденция в адрес иностранцев подлежит визированию у руководителя отдела международных связей. Один экземпляр документов остается в отделе документационного обеспечения.

Исходящая корреспонденция, адресуемая иностранцам, пишется на соответствующих бланках, на которых указаны номера телефонов, телефаксов и телексов, выделенных для работы с иностранцами. Ставить какие-либо штампы и печати на таких письмах не разрешается. Наименование отдела, фамилия и номер телефона исполнителя письма на подлиннике не указываются, а приводятся на копиях. Телексные сообщения от иностранцев принимаются отделом документационного обеспечения на специально выделенный аппарат сети Телекс.

Подготовка проектов телексных сообщений осуществляется

отделами по установленной форме на иностранном языке или клером.

Все факсимильные сообщения от иностранцев, поступающие в адрес фирмы, подлежат регистрации в отделе документационного обеспечения. Подготовка проектов факсимильных сообщений осуществляется отделами на бланках, используемых для письменной корреспонденции и со специальным титульным листом. Тексты сообщений могут быть как на русском, так и на иностранных языках. Передача телексных и факсимильных сообщений иностранцам осуществляется отделами со специально выделенными аппаратами телексной и факсимильной связи.

Сотрудники фирмы могут вести телефонные разговоры с иностранцами с телефонов, выделяемых для этих целей в каждом отделе; список телефонов подлежит согласованию с отделом международных связей и отделом технического обеспечения.

Организация работы по подготовке к выезду за границу в служебные командировки строится на основании «Временных правил оформления и выдачи заграничных паспортов гражданам РФ», утвержденных приказом МВД России № 66 от 17.02.93 г., в которых предусмотрены все процедуры оформления заграничных паспортов и получения виз для лиц выезжающих в служебные командировки.

Существуют определенные правила оформления выезда за границу. На фирме такой работой занимается отдел международных связей, который после подбора соответствующих документов на оформляемого готовит заявку по установленной форме для выезда в служебные загранкомандировки.

Соответствующее ходатайство или заявку для выезда в заграничную деловую поездку, связанную с задачами фирмы, рассматривают только в отношении работников, состоящих в штате фирмы. На ходатайстве лиц, направляемых в служебные загранкомандировки, в паспортно-визовой службе МВД России проставляется штамп «Служебная поездка». Для принятия решения о выдаче или отказе в выдаче загранпаспорта УВИР осуществляет необходимую проверку. Осведомленность лица, выезжающего за границу, в сведениях, составляющих государственную тайну, а также наличие других оснований, препятствующих выезду и относящихся к ведению органов государственной безопасности, проверяется этими органами. В процессе проверок устанавливается, не имеется ли в отношении заявителя указанных в законе ограничений, по которым ему может быть временно

отказано в выдаче загранпаспорта.

При выдаче загранпаспортов по ходатайствам ко мандирующих организаций лицам, осведомленным в сведениях, составляющих государственную тайну, руководствуются тем, что право принятия решения о выезде этих лиц в загранкомандировки предоставлено руководителям центральных органов исполнительной власти в отношении работников этих органов, а также их предприятий, учреждений и организаций. Такое право предоставлено также главам администраций краев, областей, автономных образований, городов Москвы и Санкт-Петербурга или создаваемым ими для этих целей комиссиям в отношении работников предприятий, учреждений и организаций, находящихся на этой территории, и, наконец, главам соответствующих администраций — в отношении работников этих исполнительных органов.

Организации Российской Федерации за получением въездных виз на заграничные паспорта обращаются в дипломатические представительства и консульские службы иностранных государств самостоятельно. Одновременно с оформлением виз отдел по международному сотрудничеству готовит необходимые документы, представляемые руководителю, отражающие все сведения для принятия решения загранкомандировки.

Составляется докладная записка, в которой следует указывать: цель выезда; страну командирования и принимающую организацию; срок командирования; условия финансирования поездки; фамилию, имя, отчество и занимаемую должность командируемых.

После согласования всех организационных вопросов в отношении загранкомандировки каждому члену делегации выдается техническое задание с конкретным перечнем вопросов, для решения которых организуется поездка. Технические задания составляются соответствующими отделами, согласовываются с отделом международных связей и представляются на утверждение руководству фирмы не позднее, чем за две недели до выезда. По итогам работы с иностранными делегациями и командирования за рубеж составляются отчеты, отражающие выполнение технического задания.

В процессе работы с иностранными делегациями, деловых встреч и загранкомандировок подписание каких-либо документов, которые влекут за собой экономическую или административную ответственность, выходящую за пределы компетенции предприятия, допускается только после предварительного согласо-

вания текстов *этих документов* с руководством фирмы. Отделу международных связей необходимо вести учет принимаемых иностранных делегаций и деловых встреч, а также разовых посещений иностранцами фирмы. Организацию контроля за выполнением положений настоящей Инструкции необходимо возложить на руководителей отдела международных связей и на отдел документационного обеспечения.

7.2.4. Порядок защиты конфиденциальной информации при работе с зарубежными партнерами [[^]]

Прием зарубежных партнеров, делегаций, групп должен производиться на основании «Инструкции по работе с зарубежными партнерами» и заключенных в установленном порядке международных договоров.

Вся ответственность за организацию работы с зарубежными партнерами и соблюдение требований настоящей Инструкции должны нести руководитель фирмы и руководители соответствующих отделов, отвечающие за прием иностранных представителей.

Руководители подразделений, отвечающие за организацию работы по осуществлению международных связей, обязаны:

- своевременно, в пределах своей компетенции, принимать режимные меры, гарантирующие надежную защиту;
- организовывать контроль деятельности подчиненных подразделений по организации и соблюдению режима;
- устранять выявленные в результате контроля недостатки и осуществлять мероприятия по усилению режима конфиденциальности в связи с приемом зарубежных представителей.

Основная работа по приему иностранцев ложится на специально созданные отделы — отдел по международным связям и отдел документационного обеспечения, непосредственно отвечающие за обеспечение защиты информации в этот период, и отдел, отвечающий за техническое обеспечение.

Отдел по международным связям заблаговременно

информирует о предстоящем приеме зарубежных представителей и готовит следующие документы:

- проекты планов международных связей;
- программы пребывания иностранцев в учреждении (предприятии), в том числе дополнительных мероприятий, не предусмотренных программой их пребывания.

В свою очередь отделы, отвечающие за документационное и техническое обеспечение, рассматривают проекты всех организационных документов, связанных с приемом иностранцев и другими мероприятиями по линии международного сотрудничества с целью надежной защиты коммерческой информации.

В том числе, оценивают эффективность режимных мероприятий, проводимых в отделах, намеченных для приема иностранцев, и контролируют соблюдение режимных мер в целом, и особенно в отделах, принимающих иностранцев.

Обобщают и анализируют поступающие материалы по вопросам обеспечения защиты коммерческой информации в связи с пребыванием иностранцев на объектах и в случае необходимости предпринимают меры по его усилению.

Принимают участие совместно с отделом международных связей и отделом кадров в подборе кандидатур для работы с иностранцами.

Ведут работу с лицами, имеющими непосредственное отношение к конфиденциальной информации, которые привлекаются к участию в мероприятиях по линии международного сотрудничества, с целью повышения бдительности при общении с иностранцами.

Для работы с иностранцами отдел международных связей ежегодно должен представлять списки сотрудников, выделенных для работы с зарубежными партнерами, которые затем представляются на утверждение руководителю фирмы.

Для приема иностранцев необходимо назначать ответственных лиц, которые совместно с соответствующими отделами разрабатывают программу приема иностранцев, которая затем должна быть утверждена в установленном порядке руководителем фирмы.

Программа приема иностранцев должна содержать:

- сведения о персональном составе делегации (группы) иностранцев, должностном положении ее членов и сроках ее пребывания;

- цель приема иностранцев, объем и характер информации, с которой они будут ознакомлены или которая будет передана им;
- данные о лицах, выделяемых для работы с иностранцами;
- маршрут передвижения зарубежных представителей;
- материалы и информация, которые можно использовать в беседах с иностранцами;
- порядок встречи, сопровождения и проводов иностранцев.

Для обеспечения наибольшей надежности и защиты от делам, которым поручен прием иностранцев, на основе утвержденной программы их приема необходимо разрабатывать план режимных мероприятий по обеспечению режима конфиденциальности в период пребывания иностранцев. План утверждается руководителем фирмы.

План режимных мероприятий должен предусматривать:

- мероприятия по усилению режима конфиденциальности в целом, и особенно в отделах, где будут принимать иностранцев;
- контроль в соответствии с установленными требованиями за подготовкой документации, образцов изделий и другого рода информации, ознакомление с которой или передача которой иностранцам предусматривается программой приема;
- инструктаж лиц, выделенных для работы с иностранцами;
- подготовку помещений для приема иностранцев;
- подготовку маршрута передвижения иностранцев.

Объем и характер информации, предназначенной для использования при приеме иностранцев, определяется заблаговременно в строгом соответствии с целью приема.

Переговоры, совместные научно-исследовательские, опытно-конструкторские работы и другие совместные мероприятия с зарубежными партнерами проводят в специально предназначенных или выделенных и соответствующим образом оборудованных для этих целей помещениях, по возможности изолированных от основных отделов.

В связи с этим предъявляется ряд режимных требований:

- помещения должны быть спроектированы и построены так, чтобы максимально затруднить проникновение в них посторонних лиц;
- стены и перегородки, отделяющие служебные помещения

от других помещений, должны быть выполнены из бетона, железобетона (монолитными, сборными) толщиной более 80 мм или кирпича толщиной более 120 мм;

- вышеуказанные помещения целесообразно размещать не ниже второго и не выше предпоследнего этажа;
- вблизи окон не должны проходить пожарные лестницы, водосточные трубы, козырьки, балконы и т. п., которые могли бы быть использованы для проникновения в служебное помещение;
- двери служебных помещений оборудуются надежными запорами, устройствами для опечатывания, а также устройствами для запираания;
- в служебных помещениях желательно предусматривать охранную сигнализацию, имеющую автономный источник питания и автоматическое переключение в случае выхода из строя основной системы электроснабжения. Целесообразно оборудование помещений автоматической пожарной сигнализацией.

Указанные помещения до приема иностранцев и после окончания работы с ними проверяются сотрудниками отдела технического обеспечения, в необходимых случаях должны привлекаться соответствующие специалисты.

Подготовка производственных помещений, выделенных для приема (пребывания) иностранцев, предусматривает:

- прекращение на период пребывания в этих помещениях иностранцев тех видов закрытых работ, знакомство с которыми не предусмотрено программой приема иностранцев и надежная легенда которых невозможна;
- удаление конфиденциальной документации, оборудования, материалов и других предметов, которые могут свидетельствовать о проводимых работах.

Результаты работы с иностранцами оформляются в виде письменных отчетов, записей бесед, в которых подробно излагаются обсуждавшиеся вопросы. Записи производят назначенные ответственными за прием и представляют их в отдел международных связей. При необходимости те же лица должны представлять руководителям соответствующих отделов документы, в которых отражались бы вопросы режимного характера, в том числе:

- проблемы, выходящие за рамки программы, к которым

был проявлен повышенный интерес иностранцев, и в чем это выражалось;

- возможные попытки нарушения режима пребывания и другие подозрительные действия со стороны иностранцев;
- выводы и предложения.

Подводя итог, хотелось бы еще раз сказать о том, что главной причиной, приводящей к утечке информации, составляющей коммерческую тайну, является то, что большинство сотрудников фирмы до конца не осознало, что эта информация является одним из основных ресурсов фирмы, который, как и все другие ресурсы, нуждается в защите и который нельзя растрачивать попусту. При этом следует исходить из принципиального положения, что в условиях рынка, конкуренции «закрытость» сведений выступает как элемент маркетинга и предприимчивости, как способ максимизации прибыли предприятия, создания оптимальных условий для его участия в научно-техническом прогрессе, а «открытость», бесплатный обмен «опытом работы» могут оказаться экономически опасными. От недопонимания этого происходит утечка информации по разным причинам: неумение правильно рекламировать свою продукцию, неверно понимаемый престиж и т. д.

Существует и чисто психологический аспект. Наши специалисты и инженеры, выступая на конференциях, проводя различные переговоры, рассказывают об изобретениях настолько же подробно, как они привыкли это делать на советских предприятиях. Действовать по-другому они и не могут, их этому просто не учат.

Большую роль должно сыграть воспитание и обучение сотрудников. Еще до начала переговоров сотрудник должен четко представлять, какую информацию он имеет право передавать, а что оставить «за кадром»: необходимо учить специалистов работать по принципу «черного ящика» — входные параметры изделия, полученные результаты, а как они получены — секрет фирмы. В конце концов работник должен осознавать, что от успешно проведенных переговоров зависит как благосостояние фирмы, так и его личное благосостояние.

Обеспечение защиты сведений, составляющих коммерческую тайну, должны осуществлять компетентные лица, непосредственно участвующие в коммерческой деятельности субъекта, выступающего на рынке товаров и услуг. Такие лица должны быть

специально для этого подготовлены, а их состав должен определяться руководителем фирмы.

При больших объемах коммерческой деятельности и связанных с ней сведений, составляющих коммерческую тайну, целесообразно организовать структурные подразделения, на которые возложить организацию сохранения информации предприятия, с учетом его специфики. Эти подразделения должны производить систематический анализ рынка, „... накапливать опыт участия в рыночных отношениях и на основании этого давать рекомендации по закрытию отдельных сведений или их открытию, а также поведению лиц, представляющих субъект на рынке товаров и услуг или на переговорах с другими участниками свободного рынка. Отсутствие подобных служб и их методического обеспечения является еще одной причиной утечки информации, составляющей коммерческую тайну.

Глава 8 АДУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ [^]

Доверяй, но проверяй

Аудит (контроль) состояния защиты информации — специальная проверка соответствия организации и эффективности защиты информации установленным требованиям и/или нормам.

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.

(Закон РФ «Об информации, информатизации и защите информации»)

Постулаты

1. Угрозы легче предупредить, чем устранять результаты их воздействия.
2. На бога надейся, а сам не плошай.
3. Дружба дружбой, а табачок врозь.

Проведение независимого аудита позволяет своевременно выявить существующие бреши и объективно оценить соответствие параметров, характеризующих режим информационной безопасности (ИБ), необходимому уровню. Для решения этих задач создаются специальные организации аудиторов в области информационной безопасности. Они ставят своей целью проведение экспертизы соответствия системы информационной безопасности определенным требованиям, оценки системы управления безопасностью, повышения квалификации специалистов в области информационной безопасности. Такие организации могут быть как государственными (например, подразделения государственной технической комиссии при Президенте РФ), так и иметь статус независимых, негосударственных.

Аудит позволяет оценить текущую безопасность функционирования информационной системы, оценить и прогнозировать риски, управлять их влиянием на бизнес-процессы

фирмы, корректно и обоснованно подойти к вопросу обеспечения безопасности ее информационных активов, стратегических планов развития, маркетинговых программ, финансовых и бухгалтерских ведомостей, содержимого корпоративных баз данных В конечном счете, грамотно проведенный аудит безопасности информационной системы позволяет добиться максимальной отдачи от средств, инвестируемых в создание и обслуживание системы безопасности фирмы

Основными направлениями деятельности в области аудита безопасности информации являются

- 1 Аттестация объектов информатизации по требованиям безопасности информации
 - a. аттестация автоматизированных систем, средств связи, обработки и передачи информации,
 - b. аттестация помещений, предназначенных для ведения конфиденциальных переговоров,
 - c. аттестация технических средств, установленных в выделенных помещениях
- 2 Контроль защищенности информации ограниченного доступа
 - a. выявление технических каналов утечки информации и способов несанкционированного доступа к ней,
 - b. контроль эффективности применяемых средств защиты информации
- 3 Специальные исследования технических средств на наличие побочных электромагнитных излучений и наводок (ПЭМИН)
 - a. персональные ЭВМ, средства связи и обработки информации;
 - b. локальные вычислительные системы;
 - c. оформления результатов исследований в соответствии с требованиями Гостехкомиссии России.
- 4 Проектирование объектов в защищенном исполнении.
 - a. разработка концепции информационной безопасности (первая глава учебника);
 - b. проектирование автоматизированных систем, средств связи, обработки и передачи информации в защищенном исполнении;
 - c. проектирование помещений, предназначенных для ведения конфиденциальных переговоров.

Аудит выделенных помещений

Общепринятая методика аудита выделенных помещений условно разделяет действия по выявлению средств несанкционированного съема информации (НСИ) на три этапа:

- подготовительный этап;
- этап непосредственного проведения аудита;
- заключительный этап.

Подготовительный этап аудита выделенных помещений:

- 1 Уточнение границ и ранжирование по степени важности информации, относимой к конфиденциальной.
- 2 Уточнение вероятного злоумышленника, оценка его возможностей, тактики внедрения средств НСИ и их использования.
- 3 Разработка замысла проведения аудита выделенных помещений:
 - a. выработка целевой установки;
 - b. определение масштаба и места проведения поисковых мероприятий, выбор времени проведения;
 - c. разработка легенды, под прикрытием которой будет проводиться аудит;
 - d. выработка замысла активации внедренных средств НСД;
 - e. выбор вариантов действий в случае обнаружения средств НСИ.
- 4 Изучение планов помещений, схем технических коммуникаций, связи, организации охраны, доступа и других необходимых документов.
- 5 Предварительный осмотр объекта.
- 6 Разработка перечня аппаратуры, необходимой для проведения проверки помещений и объектов.
- 7 Разработка дополнительных мер по активации внедренных средств НСИ на время проведения поиска с различными типами аппаратуры.
- 8 Распределение привлекаемых сил и средств по объектам и видам работ.
- 9 Уточнение частных методик использования привлекаемой аппаратуры в конкретных условиях

- проверки.
- 10 Оформление плана проведения комплексной проверки помещений и объектов и утверждение его у руководителя предприятия.
 - 11 Подготовка аппаратуры для проведения поисковых и исследовательских работ.
 - 12 Предварительный сбор данных и анализ радиоэлектронной обстановки в районе обследуемых объектов и помещений.
 - 13 Подготовка документов прикрытия работ по проверке помещений в соответствии с выбранной легендой прикрытия.
 - 14 Подготовка бланков, схем, заготовок других документов, необходимых для проведения работ на последующих этапах.

Перечень специального оборудования и технических средств, рекомендуемых для проведения аудита помещений.

- 1 Комплект досмотровых зеркал (ПОИСК-2, ШМЕЛЬ-2) — Визуальный осмотр оборудования, мебели, технологических коммуникаций.
- 2 Комплект луп, фонарей — Визуальный осмотр поверхностей и отверстий.
- 3 Технический эндоскоп с дистальным концом (серия ЭТ, Olympus) — Визуальный осмотр труднодоступных полостей и каналов.
- 4 Комплект отверток, ключей и радиомонтажного инструмента — Разборка и сборка коммутационных, электроустановочных и других устройств и предметов.
- 5 Досмотровый металлоискатель (УНИСКАН 7215, АКА 7202, Comet) — Проверка предметов и элементов интерьера на наличие металлических включений.
- 6 Прибор нелинейной радиолокации (NR-900EM, ОРИОН NGE-400, РОДНИК 23) — Проверка строительных конструкций и предметов на наличие радиоэлектронных компонентов.
- 7 Переносная рентгено-телевизионная установка (ШМЕЛЬ 90/К, ФП-1, РОНА) — Проверка элементов интерьера на наличие скрытно установленных средств НСИ.

- 8 Переносный радиоприемник или магнитола — Озвучивание проверяемых помещений.
- 9 Многофункциональный поисковый прибор (ПИРА-НЬЯ, ПСЧ-5, D-008) — Проверка проводных коммуникаций на наличие информационных сигналов.
- 10 Низкочастотный нелинейный детектор проводных коммуникаций (ВИЗИР, возможная замена по телефонным линиям: ТПУ-5К или SEL SP-18/Т) — Проверка проводных коммуникаций на наличие нелинейности параметров линии.
- 11 Комплекс обнаружения радиоизлучающих средств и радиомониторинга (КРОНА-6000М, КРК, АРК-Д1, OSC-5000) — Анализ радиоэлектронной обстановки, выявление радиоизлучающих средств негласного съема, информации.
- 12 Обнаружитель скрытых видеокамер (IRIS VCF-2000, нет аналогов) — Выявление радиоизлучающих видеокамер.
- 13 Дозиметр поисковый (РМ-1401, НПО-3) — Обнаружение и локализация источников радиоактивного излучения.
- 14 Комплекс для проведения исследований на сверхнормативные побочные электромагнитные излучения (НАВИГАТОР, ЛЕГЕНДА, ЗАРНИЦА) — Выявление информативных побочных электромагнитных излучений.
- 15 Комплекс для проведения акустических и виброакустических измерений СПРУТ-4А — Выявление акустических и виброакустических сигналов и наводок, исследование звуко- и виброизоляции, проверка систем шумления.

Структура плана аудита помещений:

- 1 выводы из оценки противника;
- 2 замысел проведения аудита помещений:
 - a. целевая установка;
 - b. перечень и краткая характеристика проверяемых помещений;
 - c. перечень запланированных для каждого помещения поисковых работ и сопутствующих исследований;
 - d. время проведения проверки;

- е. легенда, под прикрытием которой будет проводиться проверка;
 - ф. меры по активации внедренных средств НСИ;
 - г. действия в случае обнаружения средств НСИ;
- 3 привлекаемые для проведения проверки силы, технические средства и их распределение по объектам и видам работ;
 - 4 основные особенности применения технических средств, определяемые условиями проверки;
 - 5 дополнительные меры по активации внедренных средств НСИ;
 - 6 перечень подготавливаемых по результатам проверки итоговых и отчетных документов и срок их представления для утверждения.

Некоторые сложности могут возникнуть при организации предварительного сбора данных и анализа радиоэлектронной обстановки в районе обследуемых помещений. Если служба безопасности предприятия не располагает собственным постом радиомониторинга, с руководителем предприятия должно быть согласовано место и время развертывания временного пункта радиоконтроля с комплектом необходимой радиоприемной и анализирующей аппаратуры. В целях конспирации желательно, чтобы это место находилось где-нибудь за территорией предприятия, но в непосредственной близости от намеченных к проверке помещений. В качестве такого пункта мы рекомендуем использовать обычный легковой автомобиль с развернутым в нем комплексом обнаружения радиоизлучающих средств и радиомониторинга.

Итогом деятельности пункта радиоконтроля на этом этапе работ должна быть карта занятости радиоэфира в условиях обычного режима работы предприятия, база данных идентифицированных радиосигналов, а также база данных подозрительных радиоизлучений, требующих дополнительного исследования.

Работы подготовительного этапа обычно завершаются разработкой документов, подтверждающих легенду прикрытия при проведении различных видов поисковых и исследовательских работ, а также специальных бланков и заготовок документов, ускоряющих регистрацию промежуточных результатов запланированных работ. Целесообразно заранее изготовить бланки протоколов будущих измерений, схемы коммуникаций и планы

проверяемых помещений, на которые будут наноситься отметки мест обнаружения средств НСИ и подозрительных мест, журналы регистрации заводских номеров проверенного оборудования, мест установки пломб и скрытых меток, способствующих ускорению работ при последующих специальных проверках, и т.д.

Этапы непосредственного проведения аудита:

1. Визуальный осмотр ограждающих конструкций, мебели и других предметов интерьера помещений.
2. Проверка элементов строительных конструкций, мебели и других предметов интерьера помещений с использованием специальных поисковых технических средств.
3. Выполнение запланированных мер по активации внедренных средств НСИ.
4. Проверка линий и оборудования проводных коммуникаций:
 - a. линий силовой и осветительной электросети;
 - b. линий и оборудования офисной и абонентской телефонной сети;
 - c. линий селекторной связи;
 - d. линий радио трансляционной сети;
 - e. линий пожарной и охранной сигнализации;
 - f. линий системы часофикации и других проводных линий, в том числе, невыясненного назначения.
5. Исследование радиоэлектронной обстановки в проверяемых помещениях для выявления сигналов радиопередающих средств НСИ и их локализации.
6. Поиск средств негласного съема и передачи информации, внедренных в электронные приборы.
7. Исследование звукопроницаемости элементов конструкций, проверка трубопроводных и других технологических коммуникаций на наличие в них акустических и виброакустических сигналов из проверяемого помещения.
8. Исследование побочных электромагнитных излучений компьютеров, оргтехники и другого оборудования для выявления в них информативных сигналов.

Проверку проводных коммуникаций обычно начинают с поиска в них сигналов подслушивающих устройств или других средств съема информации. Для поиска таких сигналов

используется специальная аппаратура.

В случае обнаружения в линии сигнала подслушивающего устройства осуществляют тщательный визуальный осмотр доступных участков линии и всех подключенных к линии устройств, приборов, коммутационных и электроустановочных изделий. Обычно, чтобы убедиться в отсутствии в них средств НСИ, следует провести хотя бы частичную их разборку. Тщательно осматриваются подводящие провода, особенно в местах, где возможно несанкционированное подключение к ним каких-либо устройств или отводов. Перед осмотром элементов электросети фазы электросети, по возможности, обесточиваются.

В связи с повышенной информативной ценностью для противника телефонных каналов связи проверка телефонных линий и оборудования должна проводиться с особой тщательностью. Помимо традиционного поиска информативных сигналов мы рекомендуем проверять телефонные линии на наличие нелинейности их параметров и несимметрию, которые могут быть обусловлены подключением к линии средств НСИ.

Следует помнить, что индуктивные съемники информации с проводных линий не выявляются ни одним из перечисленных типов приборов. Поэтому даже применение нескольких разных по своим возможностям поисковых и анализирующих устройств все-таки не может заменить визуальный осмотр телефонных линий. Особенно детально должны быть осмотрены распределительные коробки и телефонный шкаф, поскольку там наиболее просто может быть осуществлено несанкционированное подключение к линии.

Обычно параллельно с проверкой проводных коммуникаций проводится радиомониторинг помещений для выявления информативных побочных излучений оргтехники и сигналов средств НСИ, использующих радиоканал для передачи перехваченной информации.

Одной из проблем современного радиомониторинга является выявление средств НСИ с нетрадиционными видами сигналов (например, шумоподобными сигналами с фазовой манипуляцией или сигналами со сверхширокополосной частотной модуляцией) или скачкообразным изменением несущей частоты. Существующие средства радиоконтроля не позволяют автоматически идентифицировать такие излучения с сигналами средств НСИ. В этой связи для радиомониторинга помещений наиболее подходят такие автоматизированные комплексы, которые позволяют опера-

тору в необходимых случаях самому проводить детальный анализ принимаемых сигналов.

Серьезным проблемным вопросом поисковых работ является выявление средств НСИ, внедренных противником в ПЭВМ или другие электронные приборы. Особую сложность представляет выявление таких средств, которые были внедрены в прибор заранее, до появления прибора в помещении, в условиях, позволивших закамуфлировать средства съема информации с особой тщательностью. В этой связи в важных служебных помещениях рекомендуется размещать только сертифицированные технические средства, прошедшие предварительный визуальный осмотр и специальную проверку. Напомним, что такую процедуру должны проходить не только новые электронные приборы, но и любые новые предметы и подарки, включая книги, видеокассеты, пепельницы и т.п.

В случае подозрения на возможность внедрения противником средств НСИ в ПЭВМ или другие электронные приборы следует провести детальное обследование этих приборов. Прежде всего проверяемый прибор необходимо разместить отдельно от других, подключить его к электросети и попытаться с помощью индикатора поля зафиксировать факт наличия или отсутствия радиоизлучения внедренного средства съема информации. Поиск излучения целесообразно повторить после приведения прибора в рабочее состояние (включения прибора). Затем с помощью прибора ПСЧ-5 или ему подобного следует убедиться в наличии или отсутствии сигналов, возможно передаваемых внедренным средством по проводам электрической сети или, если они есть, другим подключенным к прибору проводным линиям.

Следующая стадия обследования — разборка прибора и тщательный визуальный осмотр его содержимого. В процессе осмотра обращают внимание на наличие в приборе нестандартных или дополнительных плат, радиоэлементов, следов не фабричного монтажа. С особой тщательностью, с помощью лупы осматривают крупно габаритные детали: микросхемы, электролитические конденсаторы, мощные транзисторы, коммутационные элементы. Существенную помощь при этом могут оказать ранее сделанные фотографии расположения элементов монтажа на платах аналогичного прибора.

В отчетных документах по проведению специальной проверки помещений обычно требуется оценить возможность утечки информации по различным техническим каналам. Для этого

проводятся специальные исследования, включающие исследование ПЭМИ компьютеров и других средств оргтехники, наводок возникающих за счет ПЭМИ и взаимного влияния электромагнитных полей проводных линий, информативных сигналов в цепях заземления, виброакустических сигналов в элементах конструкции помещений и другие.

Заключительный этап работ по комплексной специальной проверке помещений заключается в обработке результатов исследований, проведении необходимых инженерных расчетов, разработке и представлении руководству отчетных и итоговых документов

Итоговым документом, завершающим работы по обследованию помещений на наличие средств НСИ является акт проведения комплексной специальной проверки помещений. Акт подписывается руководителем и членами поисковой бригады, согласовывается с руководителем организации, проводившей поисковые работы, и утверждается руководителем предприятия.

Этот документ обычно включает:

- время проведения специальной проверки;
- состав поисковой бригады;
- перечень проверенных помещений и объектов;
- перечень и объем основных поисковых работ и сопутствующих исследований;
- перечень использовавшейся поисковой и исследовательской аппаратуры;
- результаты специальной проверки;
- место обнаружения средства НСИ, их состояние и краткие характеристики;
- принятые по отношению к обнаруженным средствам меры;
- выводы из оценки существующей степени защищенности помещений и объектов от утечки конфиденциальной информации по различным каналам;
- рекомендации по повышению защищенности помещений и объектов и предотвращению съема информации по выявленным техническим каналам ее утечки.

Заключительный этап комплексной специальной проверки помещений:

1. Обработка результатов исследования, оформление протоколов измерений, регистрационных журналов,

- проведение необходимых инженерных расчетов.
2. Определение технических характеристик, потребительских свойств изъятых средств НСИ, ориентировочного времени и способов их внедрения.
 3. Составление описания проведенных работ и исследований с приложением необходимых схем и планов помещений.
 4. Разработка рекомендаций по повышению защищенности проверенных помещений и объектов:
 - составление перечня и схем выявленных технических каналов утечки информации по каждому помещению и объекту;
 - оценка степени существующей защиты каждого помещения и объекта от негласного съема информации по выявленным каналам ее утечки;
 - разработка дополнительных мер и способов защиты по каждому каналу и помещению (организационных, в том числе: режимных, инженерно-технических).
 5. Составление сводного перечня технических средств и систем, рекомендуемых к установке для защиты информации от утечки по техническим каналам.
 6. Разработка предложений по способам использования рекомендуемых технических средств и систем и объединению их в единую комплексную систему защиты информации.
 7. Составление акта проведения комплексной специальной проверки помещений.
 8. Представление итоговых и отчетных документов руководителю предприятия для утверждения.

К числу отчетных документов относится описание проведенных работ и исследований. В состав этого документа в качестве приложений входят протоки измерений, необходимые инженерно-технические выкладки, планы помещений с указанием места разрушения аппаратуры, обнаруженных средств НСИ и технических каналов утечки информации. В этих документах указывается: аппаратура, использованная для проведения измерений, ее заводские номера и даты последних проверок, методика проведения измерений уровни обнаруженных сигналов, их частоты и другие параметры.

Для руководства предприятия, заказавшего проведение комплексной специальной проверки помещений, наибольший интерес, помимо результатов поиска средств НСИ, представляют рекомендации по повышению защищенности проверенных помещений предотвращению съема информации по выявленным техническим каналам ее утечки. В зависимости объема и степени детализации эти рекомендации могут составлять отдельный отчетный документ.

Зачастую руководство предприятия ожидает от специалистов строгих количественных оценок степени защиты каждого помещения и объекта от негласного съема информации по всем выявленным каналам ее утечки. На практике такие оценки удается получить далеко не всегда, ибо они требуют проведения дополнительных исследований и расчетов, как правило, выходящих за рамки специальной проверки помещений. Обычно приходится ограничиваться указанием зон энергетической доступности источников информативных сигналов, ранжированием выявленных каналов утечки информации по степени угроз, экспертными оценками вероятности съема информации различными видами специальных технических средств и другими аналогичными показателями.

При разработке рекомендаций по перекрытию каналов утечки информации следует руководствоваться соображениями здравого смысла. Меры защиты должны быть адекватны степени угроз, в противном случае все финансовые ресурсы предприятия могут целиком уйти на создание системы защиты информации. Опытный специалист, владеющий основами системного мышления, всегда может найти такую комбинацию организационных, инженерных, технических мер и способов защиты, которая будет близка к оптимальной по универсальному критерию «эффективность стоимость».

Простой набор мер и средств защиты информации нейтрализует лишь отдельные угрозы ее безопасности, оставляя бреши в обороне. Только постоянно развивающаяся система информационной безопасности может сдерживать натиск непрерывно совершенствующихся средств и методов негласного съема информации.

Выводы

1. Аудит информационной безопасности фирмы — это

мощное средство оценки состояния защиты информации.

2. Аудит может проводиться как собственными силами СБ фирмы, так силами специальных лицензированных аудиторских фирм.
3. Регулярность, периодичность и масштабность аудита определяются реальной обстановкой общей безопасности предприятия.

Послесловие [^]

Опыт показывает, что для достижения удачных решений по защите информации необходимо сочетание правовых, организационных и технических мер. Это сочетание определяется конфиденциальностью защищаемой информации, характером опасности и наличием средств защиты. В общем случае технические меры безопасности составляют незначительную часть от общих мер защиты (правовых и организационных). Однако ни одну из них упускать нельзя. Каждая мера дополняет другую, и недостаток или отсутствие любого способа приведет к нарушению защиты ценности.

Работы по созданию системы защиты информации (СЗИ) включают в себя следующие этапы:

- анализ состава и содержания конфиденциальной информации, циркулирующей на конкретном объекте защиты;
- анализ ценности информации для предприятия (организации) с позиций возможного ущерба от ее получения конкурентами;
- оценка уязвимости информации, доступности ее для средств злоумышленника;
- исследование действующей системы защиты информации на предприятии;
- оценка затрат на разработку новой (или совершенствование действующей) системы;
- организация мер защиты информации;
- закрепление персональной ответственности за защиту информации;
- реализация новой технологии защиты информации;
- создание обстановки сознательного отношения к защите информации;
- контроль результатов разработки и прием в эксплуатацию новой системы защиты.

Изложенные этапы можно считать типовыми для процесса разработки систем защиты, так как они в значительной мере охватывают практически весь объем работ на организационном уровне.

Самым начальным, исходным шагом, направленным на развертывание работ по созданию или совершенствованию СЗИ, является разработка приказа руководителя организации

(предприятия) на проведение работ с указанием конкретного должностного лица, ответственного за создание СЗИ в целом. В приказе излагаются цели и задачи создания СЗИ в данной организации, определяются этапы и сроки их выполнения, назначаются конкретные должностные лица, ответственные за отдельные этапы, отдельные виды работ. В приказе определяется подразделение или временный творческий (научно-технический) коллектив, который будет вести работы по созданию (совершенствованию) системы.

Если к работе по созданию СЗИ будут привлекаться сторонние организации, в приказе оговаривается способ взаимодействия с ними, а также даются необходимые поручения по его обеспечению.

В соответствии со сложившейся практикой разработки сложных систем устанавливаются следующие стадии:

- предпроектирование работ (обследование и разработка технического задания);
- проектирование (разработка технического, рабочего или технорабочего проектов);
- ввод СЗИ в эксплуатацию.

Окончательное решение о стадийности проектирования разработки СЗИ определяется на стадии предпроектных работ при разработке ТЗ исходя из производственно-технических условий, экономических возможностей, особенностей СЗИ и используемых технических средств.

В ходе выполнения работ формируется:

- проектная документация — технический, рабочий или технорабочий проект (этап реализации технологии СЗИ);
- организационно-распорядительная документация (разрабатывается по всем этапам).

Одной из ответственных работ является обследование объекта защиты (предприятия, организации, фирмы, банка). На данной стадии:

- определяется категория объекта с позиций степени конфиденциальности его информации по важности, ценности и секретности;
- обследуются все информационные потоки по виду и важности информации;
- оцениваются режимы и технология обработки, передачи и хранения подлежащей защите информации;
- оцениваются технические средства обработки информации на всем технологическом цикле на предмет

их опасности и наличия ПЭМИН;

- определяются состав и содержание организационных, организационно-технических и технических мер, реализующих защитные мероприятия.

В результате проведения этих работ должны быть разработаны: информационная модель организации, структура информационных потоков, классификаторы потенциальных каналов утечки информации и аналитический обзор действующей системы защиты с оценкой ее эффективности, надежности и обеспечения ею необходимой безопасности.

Комплексный анализ полученных результатов в сочетании с инструментальным обследованием технических средств обработки информации с использованием контрольно-измерительной аппаратуры позволит выявить возможные каналы утечки информации за счет ПЭМИН, оценить способы несанкционированного доступа к техническим средствам и документам.

На этапе разработки определяются организационно-функциональная схема СЗИ, порядок и правила работы сотрудников в новых условиях. Предлагаемый к внедрению проект СЗИ подлежит изучению руководством организации и последующей его защите. После этого принимается решение о внедрении разработки в практику деятельности организации. Эту работу обычно выполняет группа ревизии, приема и контроля.

По завершении всех конструкторских работ СЗИ принимается в опытную эксплуатацию.

Опытная эксплуатация имеет целью отработку взаимодействия подразделений и служб в условиях новой технологии, отладку технологического процесса обработки информации и проверку соответствия реализованных решений требованиям технического проекта. Опытная эксплуатация проводится на реальных информационных потоках в соответствии с установленным регламентом.

Завершающей стадией является прием СЗИ в промышленную эксплуатацию. Для этого создается специальная приемная комиссия. Комиссия составляет акт приемки, в котором дается характеристика средствам и мерам защиты, фиксируется их полнота и достаточность, обеспечивающая требуемую степень безопасности. Акт утверждается руководством. На основании акта готовится приказ по организации на ввод СЗИ в промышленную эксплуатацию.

Порядок действий по обеспечению безопасности промышленной и коммерческой информации с детальным изложением решаемых вопросов, ответственности по их решениям, необходимых мероприятий, учитывающих специфические особенности и содержание конкретных разрабатываемых документов по основным этапам разработки, приведен в таблице 19.

Таблица содержит в основном организационные мероприятия, содержащие основные направления действий по разработке и обеспечению функционирования СЗИ. Следует отметить, что хотя этот порядок и типовой, но он носит рекомендательный характер и не претендует на нормативный материал.

Независимо оттого, насколько хорошо разработаны технические и организационные меры безопасности, они в конце концов основываются на человеческой деятельности, в которой возможны ошибки и злой умысел. Если отдельный сотрудник обманет доверие, то никакая система безопасности и секретности не сможет предотвратить неправомерное овладение информацией.

Для обеспечения уверенности в том, что данная организация успешно поддерживает функционирование системы безопасности, применяются различные методы проверки. Это регулярные независимые инспекции и ревизии, а также проверочные комиссии, включающие представителей всех участвующих в работе с конфиденциальной информацией.

Так как ни одна из форм не является идеальной, то общий контроль за деятельностью системы защиты и ее функционированием должен осуществлять высший орган

ПОРЯДОК ДЕЙСТВИЙ ПО ОБЕСПЕЧЕНИЮ

| Этапы | 1. АНАЛИЗ состава и содержания конфиденциальной информации | 2. АНАЛИЗ ценности информации | 3. ОЦЕНКА уязвимости информации | 4. ИССЛЕДОВАНИЕ действующей системы защиты информации | 5. ОЦЕНКА затрат на разработку новой системы защиты информации |
|--|--|--|---|--|--|
| Какие вопросы надо решать? | Какие сведения следует охранять? Кого интересуют охраняемые сведения и когда? Почему они нужны в получении этих сведений? | Какие виды информации имеются? Какова ценность каждого вида информации? Какая защита необходима для каждого вида информации? | Какие каналы утечки информации имеются? Какова степень уязвимости каналов утечки? Насколько уязвима информация при использовании системы и средств защиты? | Какие меры безопасности используются? Какой уровень организации защиты информации? Какова стоимость доступных мер защиты информации? Какова эффективность действующей системы защиты информации? | Какова стоимость новой системы защиты? Какой уровень организации новой системы? Какая стоимость доступа и какая велика? Какой выигрыш будет получен при новой системе? |
| Ответственные исполнители | Руководство организации, предприятия | Администрация | Специалисты отдела безопасности | Администрация, линейное руководство, отдел безопасности | Администрация, финансово-плановая служба |
| Какие мероприятия необходимо провести? | Обеспечить изучение вопросов состояния секретности и защиты информации. Составить подробный обзор всех информационных потоков. Проверить обоснованность и необходимость информационных потоков | Установить правовые и законодательные требования. Разработать принципы определения ценности информации. Определить ценность каждого вида информации | Составить перечень каналов утечки информации. Составить перечень уязвимых помещений. Установить приоритеты информации и определить охраняемые сведения. Классифицировать информацию по приоритетам и ценности | Составить аналитический обзор действующей системы защиты информации. Оценить затраты и степень риска при действующей системе защиты информации | Разработать план реализации замысла на создание новой системы защиты информации. Изыскать необходимые ресурсы |
| Что особенно нужно учитывать? | Оценить необходимость накопленной информации | Законодательную ответственность администрации за безопасность информации. Степень ущерба при раскрытии, потере, ошибках в информации. Наличие нормативных документов | Распределение приоритетов информации, требующей защиты, путем определения относительной уязвимости и степени секретности | Усиление безопасности не остановит злоумышленника. Что новая технология может быть эффективнее по критерию эффективность/стоимость | Установить требования по финансированию и его источнику |
| Какие документы разрабатываются? | Информационная модель организации, предприятия | Структура классификации информации. Принципы классификации информации. Законодательные требования, инструкции, нормы | Классификатор информации. Классификатор каналов утечки информации. | Аналитический обзор действующей СЗИ и ее безопасность | Средства СЗИ. Бюджет на разработки. Внедрение и сопровождение новой СЗИ. |

ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Таблица 19

| 6. ОРГАНИЗАЦИЯ мер защиты информации | 7. ЗАКРЕПЛЕНИЕ персональной ответственности за защиту информации | 8. РЕАЛИЗАЦИЯ технологии защиты информации | 9. СОЗДАНИЕ обстановки сознательного отношения к защите информации | 10. КОНТРОЛЬ И ПРИЕМ в эксплуатацию новой системы защиты |
|---|--|---|---|---|
| Какие появляются новые функции? Какой потребуются новый персонал? Какая квалификация необходима для выполнения новых обязанностей? | Какие конкретные сотрудники имеют доступ к охраняемым сведениям? Проверены ли эти сотрудники на благонадежность? | Каков приоритет секретной информации и изделия? Какие дополнительные ресурсы потребуются? Кто отвечает за согласование проекта СЗИ с партнерами? Замысел реализации проекта | Ориентирована ли политика организации на защиту информации? Имеется ли программа подготовки и обучения сотрудников организации в новых условиях работы с СЗИ? | Какой должен быть состав специальной группы приема системы? Имеются ли стандарты безопасности и секретности информации? Насколько эффективна новая система защиты информации? Какие улучшения можно произвести? |
| Администрация, линейное руководство, отдел безопасности | Линейное руководство, отдел безопасности | Администрация, группа реализации проекта, отдел безопасности, линейное руководство | Линейное руководство, отдел безопасности, ответственные за безопасность информации | Группа ревизии, приема и контроля работы СЗИ |
| Определить ответственность за безопасность информации в каждом подразделении. Подготовить инструкции по организации защиты информации | Проверить персонал, обрабатывающий информацию. Подготовить перечни секретных сведений для всех сотрудников | Разработать планы реализации проекта новой системы защиты информации. Определить контрольные сроки и позиции их выполнения | Разработать программы подготовки сотрудников. Оценить личные качества сотрудников по обеспечению безопасности информации | Утвердить состав группы ревизии. Рассмотреть законодательные требования. Переоценить уязвимость информации и степень риска. Оценить точность и полноту реализации проекта |
| Важность организационных мер защиты информации | Необходимость регулярного контроля за работой системы защиты информации | Полноту реализации требований новой системы защиты информации | Необходимость комплексной защиты информации. Сознательное отношение к защите информации и бдительность всего персонала | Оценить реальную эффективность новой системы защиты. Необходимость систематического контроля за работой СЗИ |
| Организационно-функциональная схема СЗИ. Порядок и правила работы в новых условиях | Профили секретности сотрудников и линейных подразделений | Подробный бюджет проекта новой СЗИ | Руководство по защите конфиденциальной информации | Программа обучения сотрудников. Отчет и рекомендации, выработанные группой ревизии |

руководства организации (предприятия) через специальные подразделения обеспечения безопасности.

- Оценка эффективности защиты должна осуществляться в соответствии с принципом комплексности и включать:
- установление на основе комплексного подхода состава проверяемых мер и средств: воспрещения, исключения несанкционированного доступа, режим;
- проверку организационно-режимных мероприятий;
- проверку категории объекта;
- проверку эффективности защиты информации;
- проверку воспрещения несанкционированного доступа;
- составление акта комплексной проверки;
- разработку рекомендаций по совершенствованию защиты (устранению установленных в процессе контроля недостатков).

На конкретных объектах при контроле эффективности защиты, обеспечиваемой конкретными СЗИ, может иметь место значительное разнообразие задач проверки. Так, на одном объекте может быть достаточно осуществить проверку эффективности экранирования, на другом — проверить эффективность шумовой защиты, а на третьем — необходимо убедиться, что излучения ПЭМИН могут быть приняты за пределами охраняемой территории организации (предприятия). То же имеет место и при проверке эффективности защиты информации от несанкционированного доступа: на одном объекте используется, например, монопольный режим обработки подлежащей защите информации, а на другом — программная система защиты информации. Все это означает, что работа по контролю эффективности защиты должна начинаться с определения состава проверяемых мер и средств. Кроме того, организационно-режимные средства и мероприятия должны иметь преимущественное значение по отношению к другим мерам и средствам защиты, поскольку их состав и эффективность оказывают определяющее действие на эффективность защиты от несанкционированного доступа. Это связано с тем, что при неправильном определении степени конфиденциальности защищаемой информации может оказаться неэффективным как воспрещение, так и защита от НСД. Иначе говоря, необходимо начинать контроль эффективности защиты с контроля организационно-режимных мер и средств защиты. Далее последовательность проверки может быть произвольной. Работы по проверке эффективности

противодействия и защиты от НСД проводятся параллельно, поскольку на практике могут осуществляться только разными группами специалистов.

Организация и проведение контроля организационных мероприятий осуществляется с целью выявления нарушений требований соответствующей инструкции по обеспечению режима, которая действует на данном объекте, а также того, как данная инструкция и действующие по ней исполнители предотвращают возникновение нарушений. При подготовке к проверке целесообразно на основе анализа составить перечень возможных нарушений, что может оказать существенную помощь в организации контроля.

Эффективность защиты объекта обеспечивается, как известно, в соответствии с категорией его важности. В свою очередь, категория важности определяется в соответствии с грифом защищаемой информации. Поэтому после проведения организационно-режимных мероприятий (работ по проверке точности установления грифа защищаемой информации) можно провести проверку правильности категорирования объекта. Если при этом категория объекта оказалась неправильно определенной (заниженной), а защита на объекте реализована в точном соответствии с категорией, то защиту следует считать неэффективной.

Контроль эффективности защиты информации от утечки за счет ПЭМИН предусматривает проведение работ с использованием определенной контрольно-измерительной аппаратуры в соответствии с существующими методиками. Этот контроль имеет целью определить наличие каналов утечки информации и их уровень за пределами охраняемой территории объекта.

Особое внимание при оценке эффективности системы защиты техническими средствами необходимо обратить на их надежность и безотказность. При их эксплуатации имеют место поломки, сбои, отказы, вследствие чего они не обеспечивают выполнение задачи защиты. Отсюда задача обеспечения надлежащей надежности технических средств обретает значительную важность, так как уровень, качество и безопасность защиты находятся в прямой зависимости от надежности технических средств.

Приложение 1

Гостехкомиссия России. Руководящий документ Защита от несанкционированного Доступа к информации. Термины и Определения

Приложение 2

Доктрина информационной безопасности Российской Федерации

Приложение 3

Перечень сведений, отнесенных к государственной тайне. Указ президента российской федерации о перечне сведений, отнесенных к государственной тайне. 24 января 1998 года № 61

Приложение 4

Указ президента российской федерации. Об утверждении перечня сведений конфиденциального характера

Приложение 5

Положение о лицензировании деятельности по технической защите конфиденциальной информации. Постановление Правительства Российской Федерации от 30 апреля 2002 г. № 290 г. Москва

Приложение 6

ИНСТРУКЦИЯ

по защите конфиденциальной информации при работе с
зарубежными партнерами

1. Общие положения

1.2. Настоящая Инструкция определяет порядок работы с зарубежными партнерами. Положениями настоящей Инструкции необходимо руководствоваться также и при контактах с представителями совместных предприятий и с представителями конкурирующих фирм и организаций.

1.3. При работе с зарубежными партнерами также следует руководствоваться положениями «Инструкции по защите коммерческой тайны».

1.4. Инструкция устанавливает режим работы с иностранцами с целью защиты конфиденциальной информации.

1.5. Под работой с иностранцами следует понимать совокупность всех видов деятельности при контактах с иностранными компаниями, фирмами (переписка, телефонные разговоры, передача телексных и факсимильных сообщений) либо личных встреч с их представителями по служебным делам.

1.6. Ответственность за организацию работы с зарубежными партнерами и соблюдение требований настоящей Инструкции несут руководство, служба безопасности и руководители соответствующих структурных подразделений фирмы.

1.7. Для работы с зарубежными партнерами ежегодно составляются списки сотрудников, выделенных для этой работы.

2. Основания для работы с зарубежными партнерами

2.2. Основанием для работы с зарубежными партнерами по служебной необходимости являются: планы международных научно-технических связей, заключенные контракты и протоколы, соглашения об установлении прямых производственных, научно-технических связей, решения о совместной деятельности, а также инициатива самих зарубежных представителей и представителей российской стороны.

2.3. Решение о приеме иностранцев принимается генеральным директором или его заместителями по представлениям

руководителей структурных подразделений, согласованных с отделом по международным связям, службой безопасности, техническим отделом и отделом документационного обеспечения.

2.4. Основанием для командирования сотрудников за рубеж служит решение генерального директора или его заместителей, выносимое на основании представляемых руководителями соответствующих отделов материалов, оформленных в установленном порядке. Принятое решение излагается письменно непосредственно на докладной записке, представляемой в установленные сроки.

2.5. В докладной записке отражаются следующие сведения: цель выезда; страна командирования и принимающая организация (фирма); срок командирования; условия финансирования поездки; фамилия, имя, отчество и занимаемая должность командироваемых.

3. Формы работы с зарубежными партнерами

3.1. Прием зарубежных делегаций

3.1.1. Прием приглашенных зарубежных делегаций осуществляется на основе утвержденных программ, составляемых по установленной форме, а также сметы расходов по приему.

Программы пребывания приглашенных зарубежных делегаций и сметы расходов составляются соответствующими подразделениями, отвечающими за прием, согла совываются с отделом международных связей, службой безопасности и утверждаются генеральным директором.

Ответственным за выполнение программы пребывания иностранной делегации является руководитель соответствующего отдела.

3.2. Организация деловых встреч (переговоров)

3.2.1. Деловые встречи с зарубежными партнерами организуются на основе заявок, оформленных соответствующими отделами, отвечающими за прием по установленной форме.

3.2.2. Заявки согласовываются с руководителем отдела международных связей, службой безопасности, отделом технического обеспечения и утверждаются генеральным директором или его заместителями.

3.2.3. Переводчиков на деловые встречи приглашает отдел, принимающий зарубежных представителей.

3.2.4. Для участия в деловых встречах с зарубежными партнерами, как правило, привлекаются специалисты из числа

сотрудников, выделенных для работы с зарубежными представителями, в количестве не менее двух человек.

3.2.5. Деловые встречи могут проводиться в кабинете генерального директора, кабинете его первого заместителя и специально выделенном для этого помещении.

3.2.6. Встречу, сопровождение и проводы зарубежных партнеров осуществляют сотрудники соответствующих отделов и отдела по международным связям.

3.2.7. Лица, участвующие в переговорах, обязаны:

- хранить конфиденциальную информацию фирмы;
- не входить в обсуждение вопросов, не относящихся к их компетенции.

3.3. Посещение приемов, симпозиумов, семинаров, выставок и других мероприятий, организуемых зарубежными партнерами или с их участием

3.3.1. Сотрудники фирмы посещают приемы, симпозиумы и семинары, организуемые зарубежными партнерами или с участием зарубежных партнеров, по служебным вопросам по согласованию с отделом международных связей, отделом технического обеспечения и с разрешения генерального директора.

3.3.2. При поступлении письменных или устных приглашений на подобные мероприятия непосредственно в адрес сотрудников следует руководствоваться п. 3.3.1. настоящей Инструкции.

3.4. Передача материалов зарубежным представителям

Передача зарубежным партнерам научно-технических и других материалов допускается после их предварительного рассмотрения руководством и службой безопасности с целью определения возможности их передачи.

3.5. Ведение служебной переписки. Прием и передача телексных и факсимильных сообщений, ведение телефонных разговоров с зарубежными партнерами.

3.5.1. Общие положения:

3.5.1.1. Руководство фирмы, отделы и подразделения фирмы ведут служебную переписку, прием и передачу телексных и факсимильных сообщений через отдел документационного обеспечения.

3.5.1.2. Вся входящая международная корреспонденция (вне зависимости от ее вида) регистрируется и первично рассматривается в отделе документационного обеспечения. Корреспонденция

докладывается генеральному директору или его заместителям или направляется на рассмотрение и исполнение непосредственно в отделы.

3.5.1.3. После рассмотрения руководством корреспонденция в соответствии с резолюцией направляется исполнителям, и контроль за сроками исполнения поручения осуществляется в соответствии с установленным порядком.

3.5.1.4. Право подписи корреспонденции в адрес зарубежных представительств имеют генеральный директор, его заместители и начальники отделов.

3.5.1.5. Любая корреспонденция в адрес зарубежных представительств подлежит визированию у руководства и в службе безопасности фирмы. Один экземпляр документов остается в отделе документационного обеспечения.

3.5.2. Работа с письмами

3.5.2.1. Служебные письма, адресуемые зарубежным партнерам, пишутся на фирменных бланках с указанием наименования фирмы на английском языке, а также с разрешенными номерами телефонов, факсов и телексов, выделенных для работы с зарубежными представителями. Ставить какие-либо штампы и печати на таких письмах не разрешается.

3.5.2.2. Проекты писем в адрес зарубежных партнеров готовятся в отделах фирмы при строгом соблюдении конфиденциальности. Наименование отдела, фамилия и номер телефона исполнителя письма на подлиннике не указываются, а приводятся на копиях.

3.5.3. Работа с телексными сообщениями

3.5.3.1. Телексные сообщения от иностранцев принимаются на специально выделенный аппарат сети Телекс.

3.5.3.2. Подготовка проектов телексных сообщений осуществляется отделами по установленной форме на иностранном языке.

3.5.3.3. Отправка телексных сообщений зарубежным партнерам осуществляется в порядке, установленном настоящей Инструкцией.

3.5.4. Работа с факсимильными сообщениями

3.5.4.1. Все факсимильные сообщения от иностранцев подлежат регистрации в отделе

документационного обеспечения.

3.5.4.2. Подготовка проектов факсимильных сообщений осуществляется отделами на бланках, используемых для письменной корреспонденции и со специальным титульным листом. Тексты сообщений могут быть как на русском, так и на иностранных языках. Требования к реквизитам исполнителя аналогичны требованиям п. 3.5.2.2. настоящей Инструкции.

3.5.4.3. Передача факсимильных сообщений иностранцам осуществляется отделами со специально выделенного аппарата факсимильной связи с предварительной регистрацией в отделе документационного обеспечения.

3.5.5. Ведение телефонных разговоров Сотрудники фирмы могут вести телефонные разговоры с зарубежными партнерами с телефонов, выделяемых для этих целей в каждом отделе: список телефонов подлежит согласованию с отделом международных связей и службой безопасности.

3.6. Командирование за рубеж

3.6.1. Состав делегаций, командируемых за рубеж за счет собственных средств, формируется соответствующими отделами и согласовывается с отделом международных связей, службой безопасности и руководством фирмы.

3.6.2. При командировании за рубеж по служебной линии делегациям и отдельным специалистам выдается техническое задание, в котором отражается перечень конкретных вопросов, для решения которых организуется поездка.

Технические задания составляются отделом международных связей и представляются на утверждение руководству не позднее чем за две недели до выезда.

3.6.3. Оформление выездных документов производится в отделе международных связей в установленном порядке.

4. Оформление результатов работы с иностранцами, учет и отчетность

4.1. Соответствующие отделы, принимающие иностранцев, по итогам работы с зарубежными партнерами и командирования за рубеж составляют отчеты произвольной формы. По итогам деловых встреч составляются записи бесед по установленной форме. Записи бесед представляются в отдел по международным связям в двухдневный срок после окончания работы с

иностранцами, а отчеты, как правило, — в двухнедельный срок (два печатных экземпляра).

4.2. В записях бесед и отчетах указывается: когда, где, с кем состоялась встреча; ее основание и цель; кем дано разрешение на встречу, какое учреждение, организацию или фирму представляли иностранцы, их фамилии и должностное положение; кто присутствовал со стороны фирмы; содержание беседы (существо вопросов и ответы на них); какая документация и какие образцы изделий и материалов переданы зарубежным представителям или получены от них, обязательства сторон по существу обсуждавшихся вопросов, а также другая заслуживающая внимания информация.

4.3. Отдел международных связей ведет учет принимаемых иностранных делегаций и деловых встреч, а также учет сообщений от фирмы о контактах с иностранцами.

5. Организационные мероприятия по результатам работы с иностранцами

5.1. Отчеты по результатам работы с зарубежными представительствами и записи бесед, содержание обязательства и предложения сторон докладываются со ответственными отделами, организовавшими встречу, руководству фирмы и службе безопасности.

5.2. Координация работ по выполнению поручений руководства по данным документам возлагается на отдел международных связей и службу безопасности.

5.3. Контроль за выполнением положений настоящей Инструкции возлагается на руководство фирмы, отдел международных связей и службу безопасности.

Приложение 7

ОБЕСПЕЧЕНИЕ СОХРАНЕНИЯ КОММЕРЧЕСКОЙ ТАЙНЫ ПРЕДПРИЯТИЯ

Введение

Важными источниками конфиденциальной информации являются люди, документы и публикации. От того, как организована работа с людьми и документами, зависит и безопасность предприятия. Целям предотвращения нанесения экономического, финансового и материального ущерба предприятию (организации), вызванного неправомерными или неосторожными действиями, а также неквалифицированным обращением или разглашением коммерческой тайны, служат настоящие предложения.

Предложения по обеспечению коммерческой тайны носят общий рекомендательный характер, не являются нормативным документом, ориентированы в основном на работу с документами, содержащими сведения коммерческого характера, и предусматривают главным образом организационные меры защиты коммерческих секретов.

При подготовке данного пособия были использованы материалы и опыт государственных и коммерческих структур по защите информации.

1. Общие положения

1.1. Под коммерческой тайной понимаются не являющиеся государственными секретами сведения, связанные с производственно-технической, научно-исследовательской, опытно-конструкторской и другой деятельностью предприятия, а также с их технологической информацией, управлением, финансами, разглашение, утечка или неправомерное овладение которыми может нанести ущерб его интересам.

1.2. К сведениям, составляющим коммерческую тайну, относятся несекретные сведения, предусмотренные «Перечнем конкретных сведений, составляющих коммерческую тайну», утвержденным и введенным в действие приказом директора предприятия.

Коммерческая тайна является собственностью предприятия.

Если коммерческая тайна является результатом совместной деятельности с другими предприятиями, основанной на договорных началах, то коммерческая тайна может быть собственностью двух сторон. Это обстоятельство должно найти отражение в договоре.

Примечание. Единой установки на обозначение грифа ограничения доступа к документу, содержащему коммерческую тайну, нет, таким грифом может быть «коммерческая тайна». На других предприятиях могут быть: «коммерческая тайна», «секрет предприятия», «тайна предприятия» и др. Такой ограничительный гриф не является грифом секретности, а лишь показывает, что право собственности на данную информацию охраняется законодательством

1.3. Под разглашением коммерческой тайны имеются в виду противоправные, умышленные или неосторожные действия должностных или иных лиц, приведшие к преждевременному, не вызванному служебной необходимостью, оглашению охраняемых сведений, подпадающих под эту категорию, а также передача таких сведений по открытым техническим каналам или обработка их на некатегоризированных ЭВМ.

1.4. Под открытым опубликованием вышеуказанных сведений имеется в виду публикация материалов в открытой печати, передача по радио и телевидению, оглашение на международных, зарубежных и открытых внутренних съездах, конференциях, совещаниях, симпозиумах, при публичной защите диссертаций и других публичных выступлениях, свободная рассылка, вывоз материалов за границу или передача их в любой форме иностранным фирмам, организациям или отдельным лицам вне сферы прямых служебных обязанностей.

1.5. Необходимость и возможность открытого опубликования этих сведений, а также их объемы, формы и время опубликования определяются директором или его заместителями по направлениям по заключению постоянно действующей экспертной комиссии.

1.6. Меры по ограничению открытых публикаций коммерческой информации не могут быть использованы во вред принципу гласности и для сокрытия от общественности фактов бесхозяйственности, расточительства, недобросовестной конкуренции и других негативных явлений.

Использование для открытого опубликования сведений, полученных на договорной или доверительной основе или

являющихся результатом совместной производственной деятельности, допускается лишь с общего согласия партнеров.

1.7. Передача информации сторонним организациям, не связанным прямыми служебными контактами, должна регулироваться, как правило, договорными отношениями, предусматривающими обязательства и ответственность пользователей, включая возмещение материальных затрат на предоставление информации и компенсацию за нарушение договорных обязательств.

1.8. Предоставление коммерческой информации представителям служебных, ревизионных, фискальных и следственных органов, народным депутатам, органам печати, радио регулируется соответствующими положениями.

1.9. Тиражированные документы и издания с грифом «коммерческая тайна» рассматриваются как материалы, содержащие сведения ограниченного распространения.

1.10. Ответственность за обеспечение режима при работе с материалами с грифом «КТ», своевременную разработку и осуществление необходимых мероприятий по сохранению коммерческой тайны возлагается на директора, его заместителей по направлениям и руководителей структурных подразделений. Ответственность за организацию и осуществление работы по защите коммерческой тайны и проведение постоянного контроля за ее соблюдением возлагается на службу безопасности.

Служба безопасности принимает меры по сохранению коммерческой тайны путем максимального ограничения круга лиц, физической сохранности документов, содержащих такие сведения, обработки информации с грифом «КТ» на защищенных ЭВМ, внесения требований по конфиденциальности конкретной информации в договоры с внутренними и внешнеторговыми партнерами и других мер по решению руководства.

1.11. Защита коммерческой тайны предусматривает:

- порядок определения информации, содержащей коммерческую тайну, и сроков ее действия;
- систему допуска сотрудников, командированных и частных лиц к сведениям, составляющим коммерческую тайну;
- порядок работы с документами с грифом «КТ»;
- обеспечение сохранности документов, дел и изданий с грифом «КТ»;
- обязанности лиц, допущенных к сведениям, состав-

ляющим коммерческую тайну;

- принципы организации и проведения контроля за обеспечением режима при работе со сведениями, составляющими коммерческую тайну;
- ответственность за разглашение сведений, утрату документов, содержащих коммерческую тайну.

1.12. Контроль за осуществлением учета, размножением, хранением и использованием документов, дел и изданий с грифом «КТ» возлагается на уполномоченных службы безопасности.

1.13. Контроль за неразглашением сведений, содержащихся в документах, делах и изданиях с грифом «КТ», осуществляется отделами службы безопасности.

2. Порядок определения информации, содержащей коммерческую тайну, и сроков ее действия

2.1. Определение необходимости проставления грифа «коммерческая тайна» производится на основании Перечня, указанного в п. 1.2: на документе — исполнителем и лицом, подписывающим документ, а на издании — автором (составителем) и руководителем, утверждающим издание к печати.

2.2. Срок действия коммерческой тайны, содержащейся в документе, определяется в каждом конкретном случае исполнителем или лицом, подписавшим документ, в виде конкретной даты, или «до заключения контракта», или «бессрочно».

2.3. На документах, делах и изданиях, содержащих сведения, составляющие коммерческую тайну, проставляется гриф «коммерческая тайна», а на документах и изданиях, кроме того, — номера экземпляров.

Гриф «коммерческая тайна» и номер экземпляра проставляются в правом верхнем углу первой страницы документа, на обложке, титульном листе издания и на первой странице сопроводительного письма к этим материалам.

На обратной стороне последнего листа каждого экземпляра документа, содержащего коммерческую тайну, печатается разметка, в которой указывается: количество отпечатанных экземпляров, номер, фамилия исполнителя и его телефон, дата, срок действия коммерческой тайны, содержащейся в документе (конкретная дата, «до заключения контракта» или «бессрочно»), фамилия машинистки.

2.4. Решение вопроса о снятии грифа «коммерческая тайна»

возлагается на создаваемую в установленном порядке специальную комиссию, в состав которой включаются представители службы безопасности и соответствующих структурных подразделений.

Решение комиссии оформляется составляемым в произвольной форме актом, который утверждается директором или его заместителем по направлению. В акте перечисляются дела, с которых гриф «КТ» снимается. Один экземпляр акта вместе с делами передается в архив, а на дела постоянного хранения — в государственный архив.

2.5. На обложках дел гриф «КТ» погашается штампом или записью от руки с указанием даты и номера акта, послужившего основанием для его снятия.

Аналогичные отметки вносятся в описи и номенклатуры дела.

3. Система допуска сотрудников, командированных и частных лиц к сведениям, составляющим коммерческую тайну

3.1. Допуск сотрудников к сведениям, составляющим коммерческую тайну, осуществляется директором, его заместителями по направлениям и руководителями структурных подразделений.

Руководители подразделений и службы безопасности ответственны за подбор лиц, допускаемых к сведениям с грифом «КТ», обязаны обеспечить систематический контроль за тем, чтобы к этим сведениям получали доступ только те лица, которым такие сведения необходимы для выполнения своих служебных обязанностей.

3.2. К сведениям, составляющим коммерческую тайну, допускаются лица, обладающие необходимыми высоконравственными и деловыми качествами, способные хранить коммерческую тайну, и только после оформления в службе безопасности индивидуального письменного обязательства по сохранению коммерческой тайны.

3.3. Допуск сотрудников к работе с делами с грифом «КТ», имеющих к ним непосредственное отношение, производится в соответствии с оформленным на внутренней стороне обложки списком за подписью руководителя структурного подразделения, а к документам — согласно указаниям, содержащимся в резолюциях руководителей подразделений.

3.4. Командированные и частные лица допускаются к ознакомлению и работе с документами и изданиями с грифом «КТ»

с письменного разрешения руководителей предприятия и подразделений, в ведении которых находятся эти материалы, при наличии письменного запроса тех организаций, в которых они работают, с указанием темы и объема выполняемого задания, а также предписания на выполнение задания.

Выписки из документов и изданий, содержащих сведения с грифом «КТ», производятся в тетрадях, имеющих такой же гриф, и после окончания работы представителя высылаются в адрес организации.

3.5. Дела и издания с грифом «КТ» выдаются исполнителям и принимаются от них под расписку в «Карточке учета выдаваемых дел и изданий» (форма 4).

4. Порядок работы с документами с грифом «КТ»

4.1. Документы, содержащие сведения, составляющие коммерческую тайну, подлежат обязательной регистрации в канцелярии службы безопасности или в общем делопроизводстве подразделения уполномоченным службы безопасности. Они должны иметь реквизиты, предусмотренные п. 2.3, и гриф «КТ» (или полностью «коммерческая тайна»). На документах, передаваемых иностранцам, гриф «КТ» не проставляется. Полученные от иностранцев документы маркируются грифом «КТ» графитным карандашом.

В тексте документа и его реквизитах дополнительно могут оговариваться права на информацию, порядок пользования ею, сроки ограничения на публикацию и др.

Отсутствие грифа «КТ» и предупредительных оговорок в тексте и реквизитах означает свободную рассылку и предполагает, что автор информации и должностное лицо, санкционирующее (подписавшее, утверждавшее документ) ее распространение, предусмотрели все возможные последствия от свободной рассылки и несут за это всю полную ответственность.

4.2. Вся поступающая корреспонденция с грифом «КТ» или другими грифами, указанными в п. 1.2, принимается и вскрывается сотрудниками канцелярии, которым поручена работа с этими материалами. При этом проверяется количество листов и экземпляров документов и изданий, а также наличие указанных в сопроводительном письме приложений.

В случае отсутствия в конвертах (пакетах) документов «КТ» или приложений к ним составляется акт в двух экземплярах, один из которых отправляется адресату.

4.3. Регистрации подлежат все входящие, исходящие и внутренние документы, а также издания с грифом «КТ». Такие документы учитываются по количеству листов, а издания (книги, журналы, брошюры) — поэкземплярно.

4.4. Учет документов и изданий с грифом «КТ» ведется в журналах (форма 1) или на карточках (форма - 2) отдельно от учета другой несекретной документации.

Листы журналов нумеруются, прошиваются и опечатываются. Издания, которые не подшиваются в дела, учитываются в журнале инвентарного учета (форма 5).

Движение документов и изданий с грифом «КТ» должно своевременно отражаться в журналах или на карточках.

4.5. На каждом зарегистрированном документе, а также на сопроводительном листе к изданиям с грифом «КТ» проставляется штамп, в котором указываются наименование, регистрационный номер документа и дата его поступления.

4.6. Тираж издания с грифом «КТ», полученный для рассылки, регистрируется под одним входящим номером в журнале учета и распределения изданий (форма 3).

Дополнительно размноженные экземпляры документа (издания) учитываются за номером этого документа (издания), о чем делается отметка на размножаемом документе (издании) и в учетных формах. Нумерация дополнительно размноженных экземпляров производится от последнего номера ранее учтенных экземпляров.

4.7. Печатаение материалов с грифом «КТ» производится в бюро оформления технической документации или в структурных подразделениях под ответственность их руководителей.

4.8. Отпечатанные и подписанные документы с грифом «КТ» вместе с их черновиками и вариантами передаются для регистрации сотруднику канцелярии, осуществляющему их учет. Черновики и варианты уничтожаются этим сотрудником с подтверждением факта уничтожения записью на копии исходящего документа: «Черновик (и варианты) уничтожены». Дата. Подпись.

4.9. Размножение документов и изданий с грифом «КТ» в типографиях и на множительных аппаратах производится с разрешения службы безопасности и под контролем канцелярии по заказам, подписанным руководителем подразделения и утвержденным заместителем директора по направлению. Учет размноженных документов и изданий осуществляется поэкземплярно в специальном журнале.

4.10. Рассылка документов и изданий с грифом «КТ» осуществляется на основании подписанных руководителем структурного подразделения разнарядок с указанием учетных номеров отправляемых экземпляров.

4.11. Документы с грифом «КТ» после исполнения группируются в отдельные дела. Порядок их группировки предусматривается номенклатурами дел несекретного делопроизводства. В номенклатуру дел в обязательном порядке включаются все справочные картотеки и журналы и издания с грифом «КТ».

4.12. При пользовании открытой радиосвязью запрещается передавать сведения, имеющие гриф «КТ». Такие сведения могут передаваться только по закрытым техническим средствам связи или по открытой телетайпной связи с проставлением на документах и телеграммах соответствующего штампа.

При пользовании проводной связью запрещается указывать должности адресатов отправителей, разрешается указывать только телеграфные адреса и фамилии отправителей и получателей.

4.13. Снятие копий (рукописных, машинописных, микро- и фотокопий, электрографических и др.), а также производство выписок из документов и изданий с грифом «КТ» сотрудниками производится по разрешению руководителей подразделений.

Снятие копий для сторонних организаций с документов и изданий с грифом «КТ» производится на основании письменных запросов по разрешению руководителей подразделений, подготовивших эти документы и издания.

Аналогично отметки вносятся в описи и номенклатуры дел.

4.14. Порядок работы на ЭВМ при обработке информации с грифом «КТ» осуществляется в соответствии с требованиями «Инструкции о порядке работы на ПЭВМ при обработке несекретной информации».

5. Обеспечение сохранности документов, дел и изданий

5.1. Документы, дела и издания с грифом «КТ» должны храниться в служебных помещениях и библиотеках в надежно запираемых и опечатываемых шкафах (хранилищах). При этом должны быть созданы надлежащие условия, обеспечивающие их физическую сохранность.

5.2. Выданные для работы дела с грифом «КТ» подлежат возврату в канцелярию или уполномоченному службы безопасности в тот же день.

Отдельные дела с грифом «КТ» с разрешения начальника канцелярии или уполномоченного службы безопасности могут находиться у исполнителя в течение срока, необходимого для выполнения задания, при условии полного обеспечения их сохранности и соблюдения правил хранения.

5.3. Передача документов, дел и изданий с грифом «КТ» другим сотрудникам, допущенным к этим документам, производится только через канцелярию или уполномоченного службы безопасности.

5.4. Запрещается изъятие из дел или перемещение документов с грифом «КТ» из одного дела в другое без санкции канцелярии или уполномоченного службы безопасности, осуществляющего их учет. Обо всех проведенных изъятиях или перемещениях делаются отметки в учетных документах, включая внутренние описи.

5.5. Запрещается выносить документы, дела и издания с грифом «КТ» из служебных помещений для работы с ними дома, в гостиницах и т. д.

В необходимых случаях директор, его заместители по направлениям или руководители структурных подразделений могут разрешить исполнителям или сотрудникам канцелярии вынос из здания документов с грифом «КТ» для их согласования, подписи и т. д. в организации, находящиеся в пределах данного города.

5.6. Лицам, командированным в другие города, запрещается иметь при себе в пути следования документы, дела или издания с грифом «КТ». Эти материалы должны быть направлены заранее в адрес организации по месту командировки сотрудника, как правило, заказными или ценными почтовыми отправлениями, а также с курьерами.

5.7. При смене сотрудников, ответственных за учет и хранение документов, дел и изданий с грифом «КТ», составляется по произвольной форме акт приема-передачи этих материалов, утверждаемый заместителями директора по направлениям или руководителями структурных подразделений.

6. Обязанности лиц, допущенных к сведениям, составляющим коммерческую тайну

6.1. Лица, допущенные к работам, документам и сведениям, составляющим коммерческую тайну, несут личную ответственность за соблюдение ими установленного режима. Прежде чем получить доступ к коммерческой информации, они

должны изучить требования настоящей инструкции и других нормативных документов по защите коммерческой тайны в части, их касающейся, сдать зачет на знание указанных требований и дать индивидуальное письменное обязательство по сохранению коммерческой тайны.

6.2. Лица, допущенные к работам, документам и сведениям, составляющим коммерческую тайну, обязаны:

- а) строго хранить коммерческую тайну, ставшую им известной по службе или работе или иным путем, пресекать действия других лиц, которые могут при вести к разглашению коммерческой тайны. О таких фактах, а также о других причинах или условиях возможной утечки коммерческой тайны немедленно информировать непосредственного начальника и службу безопасности;
- б) в течение договорного периода не использовать известную коммерческую тайну в своих личных *целях*, а также без соответствующего разрешения руководства не заниматься любой деятельностью, которая в качестве конкурентного действия может нанести ущерб предприятию, являющемуся владельцем этой коммерческой тайны;
- в) выполнять только те работы и знакомиться только с теми документами, к которым получили доступ в силу своих служебных обязанностей; знать степень важности выполняемых работ, правильно определять ограничительный гриф документов, строго соблюдать правила пользования ими, порядок их учета и хранения;
- г) при составлении документов со сведениями, составляющими коммерческую тайну, ограничиваться минимальными, действительно необходимыми в документе этими сведениями; определять количество экземпляров документов в строгом соответствии с действительной служебной необходимостью и не допускать рассылки их адресатам, к которым они не имеют отношения;
- д) на черновиках документов проставлять соответствующий ограничительный гриф и другие необходимые реквизиты. Передавать их для печатания только с письменного разрешения руководителя подразделения;
- е) после получения из машинописного бюро отпечатанных документов проверять их наличие, сличать эти данные с записями в журнале и расписываться (с указанием даты) за получение отпечатанных документов и черновиков, после чего

- учесть в канцелярии или у уполномоченного службы безопасности;
- ж) получать документы с грифом «КТ» лично в канцелярии или у уполномоченного службы безопасности. Своевременно знакомиться с полученными документами и разборчиво расписываться на них с указанием даты ознакомления;
 - з) поступившие документы с грифом «КТ» своевременно направлять для приобщения к делу с соответствующими отметками об исполнении (номер дела, что сделано по документу, дата, подпись) и с резолюцией начальника подразделения;
 - и) сдавать в канцелярию или уполномоченному по службе безопасности исполненные входящие документы, а также предназначенные для рассылки, подшивки в дело, уничтожения и взятия на инвентарный учет под расписку в журналах учета;
 - к) иметь внутреннюю опись документов с грифом «КТ», в которой отводится отдельный раздел, и немедленно вносить с нее все полученные для исполнения документы, хранить их только в рабочей папке, а при выходе в рабочее время из помещения рабочую папку с документами запирать в сейф;
 - л) по окончании работы с документами с грифом «КТ» своевременно возвращать их в канцелярию или уполномоченному службы безопасности;
 - м) об утрате или недостатке документов с грифом «КТ», ключей от сейфов, личных печатей немедленно сообщать в службу безопасности;
 - н) при увольнении, перед уходом в отпуск, отъездом в командировку своевременно сдать или отчитаться перед канцелярией или уполномоченным за все числящиеся за ним документы;
 - о) ознакомить представителей других учреждений с документами с грифом «КТ» с ведома и с письменного разрешения руководителя подразделения; лично знакомиться с разрешениями указанных руководителей на предписании, в котором должны быть определены вопросы и объем сведений, подлежащих рассмотрению; требовать от командированных лиц расписки на документах, с которыми они ознакомились, или в учетных карточках этих документов;
 - п) документы с грифом «КТ» во время работы располагать так, чтобы исключить возможность ознакомления с ними других

- лиц, в том числе допущенных к подобным работам и документам, но не имеющих к ним прямого отношения;
- р) по первому требованию канцелярии и отдела службы безопасности предъявлять для проверки все числящиеся и имеющиеся документы с грифом «КТ»; представлять по требованию начальника отдела устные или письменные объяснения о нарушениях установленных правил выполнения работ с грифом «КТ», учета и хранения документов с грифом «КТ», а также о фактах разглашения сведений с грифом «КТ», утраты документов, содержащих такие сведения.

7. Принципы организации и проведения контроля за обеспечением режима при работе со сведениями, содержащими коммерческую тайну

7.1. Контроль за обеспечением режима при работе со сведениями, составляющими коммерческую тайну, осуществляется в целях изучения и оценки фактического состояния сохранности коммерческой тайны, выявления недостатков и нарушений режима при работе с материалами с грифом «КТ», установления причин таких недостатков и нарушений и выработки предложений, направленных на их устранение и предотвращение.

7.2. Контроль за обеспечением режима при работе с материалами с грифом «КТ» осуществляет служба безопасности и руководители структурных подразделений.

7.3. Комиссия для проверки обеспечения режима при работе с материалами с грифом «КТ» комплектуется из опытных и квалифицированных работников в составе не менее 2-х человек, имеющих допуск к этой работе. Участие в проверке не должно приводить к необоснованному увеличению осведомленности проверяющих об этих сведениях.

7.4. Проверки обеспечения режима при работе с материалами с грифом «КТ» проводятся не реже одного раза в год комиссиями на основании предписания, подписанного директором или его заместителем по направлению.

7.5. Проверки проводятся в присутствии руководителя структурного подразделения или его заместителя.

7.6. Проверяющие имеют право знакомиться со всеми документами, журналами (карточками) учета и другими материалами, имеющими отношение к проверяемым вопросам, а также проводить беседы и консультации со специалистами и исполнителями, требовать представления письменных объяснений,

справок, отчетов по всем вопросам, входящим в компетенцию комиссии.

7.7. По результатам проверок составляется акт (справка) с отражением в нем состояния режима при работе с материалами с грифом «КТ», выявленных недостатков и нарушений, предложений по их устранению.

С актом после утверждения его директором или заместителем под роспись знакомится руководитель структурного подразделения.

7.8. Об устранении выявленных в результате проверки недостатков и нарушений в режиме при работе с материалами с грифом «КТ» и реализации предложений руководитель подразделения в установленные комиссией сроки сообщает начальнику службы безопасности.

7.9. В случае установления факта утраты документов, дел и изданий с грифом «КТ» либо разглашения содержащихся в них сведений немедленно ставятся в известность директор, его заместители по направлениям и начальник службы безопасности.

Для расследования факта утраты документов, дел и изданий с грифом «КТ» при установлении факта разглашения сведений, содержащихся в этих материалах, приказом директора (распоряжением руководителя структурного подразделения) назначается комиссия, заключение которой о результатах расследования утверждается руководителем, создавшим данную комиссию.

На утраченные документы, дела и издания с грифом «КТ» составляется акт. Соответствующие отметки вносятся в учетные документы.

Акты на утраченные дела постоянного хранения после их утверждения директором или его заместителями по направлениям передаются в архив для включения в дело фонда.

8. Ответственность за разглашение, утрату документов, содержащим коммерческую тайну

8.1. Разглашение сведений, составляющих коммерческую тайну, — это предание огласке сведений лицом, которому эти сведения были доверены по службе, работе или стали известны иным путем, в результате чего они стали достоянием посторонних лиц.

8.2. Утрата документов, содержащих сведения коммерческой тайны, — это выход (в том числе и временный)

документов из владения ответственного за их сохранность лица, которому они были доверены по службе или работе, являющийся результатом нарушения установленных правил обращения с ними, вследствие чего эти документы стали или могли стать достоянием посторонних лиц.

8.3. Иные нарушения режима при работе с материалами коммерческой тайны — это нарушение требований, могущее привести к разглашению этих сведений, утрате документов, содержащих такие сведения.

8.4. За утрату и незаконное уничтожение документов, дел и изданий с грифом «КТ», за разглашение сведений, содержащихся в этих материалах, а также за нарушение требований виновные лица привлекаются к ответственности в установленном порядке.

Приложения:

1. Договорное обязательство
2. Форма № 1
3. Форма № 2
4. Форма № 3
5. Форма № 4
6. Форма № 5
7. Типовой договор на комплексное режимное обслуживание
8. Типовой акт приемки выполнения договорных обязательств

Договорное обязательство

Я, _____
(фамилия, имя, отчество)

оформляясь на работу, _____
(должность, подразделение)

обязуюсь:

1. в период работы не разглашать сведения, составляющие коммерческую тайну, которые мне будут доверены или станут известны при исполнении служебных обязанностей;
2. беспрекословно и аккуратно выполнять относящиеся ко мне требования приказов, инструкций и положений по защите коммерческой тайны, с которыми я ознакомлен;
3. не сообщать устно или письменно кому бы то ни было сведения, составляющие коммерческую тайну;
4. в случае увольнения не разглашать и не использовать для себя или других сведения, составляющие коммерческую тайну.

Я предупрежден, что в случае нарушения данного обязательства должен возместить ущерб или буду привлечен к дисциплинарной или уголовной ответственности в соответствии с законодательством.

(подпись)

Проинструктировал

«__» _____ 200 г.

Журнал учета документов и изданий с грифом «Коммерческая тайна»

| Порядковый номер (вход/исход) | Дата поступления и индекс документа | Дата и индекс документа | Откуда поступил или куда направлен | Наименование документа и краткое содержание | Количество листов | | Количество и номера экземпляров |
|-------------------------------|-------------------------------------|-------------------------|------------------------------------|---|-------------------|------------|---------------------------------|
| | | | | | документа | приложения | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| | | | | | | | |

(продолжение)

| Резолюция или кому направлен на исполнение | Отметка о взятии на контроль и срок исполнения | Дата и расписка | | Индекс (номер) дела, куда подшит документ | Отметка об уничтожении | Примечание |
|--|--|-----------------|------------|---|------------------------|------------|
| | | в получении | о возврате | | | |
| 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| | | | | | | |

Форма № 1

Карточка учета входящих (исходящих) документов и изданий с грифом «КТ»

| Вход. (исход.) номер и гриф | Дата регистрации | Исход. номер и дата поступившего документа | Количество листов | |
|-----------------------------|------------------|--|---------------------|------------|
| | | | основного документа | приложения |
| | | | | |

Наименование отправителя:

Краткое содержание:

| Подшивка | | | Регистрация приложения | | |
|------------|--------------|------------------------|------------------------|--------|------------------------|
| номер дела | номер листов | подписи о сверке, дата | вид | инв. № | подписи о сверке, дата |
| | | | | | |

Отметка о сверках наличия

Карточка проверена, все позиции закрыты

(подпись)

« ____ » _____ 19__ г.

(лицевая сторона)

Движение

| Дата | Количество основных приложений | Кому выдан или куда отправлен | Роспись в получении или № реестра | Подписи о сверке, дата | Дата возврата | Роспись в приеме или отм. о возврате |
|------|--------------------------------|-------------------------------|-----------------------------------|------------------------|---------------|--------------------------------------|
| | | | | | | |

Для разных отметок:

(оборотная сторона)

Карточка учета выдаваемых дел и изданий с грифом «КТ»

| № п/п | № дела, № экз. изданий и кол-во листов | Наименование дела или издания | | | | Примечание |
|-------|--|------------------------------------|--------------------|-------------------|---|------------|
| | | Подразделение и фамилия сотрудника | Расписка | | | |
| | | | в получении и дата | о возврате и дата | | |
| 1 | 2 | 3 | 4 | 5 | 6 | |

Форма № 5

Журнал учета служебных изданий с грифом «КТ»

| № п/п | Дата и № сопроводительного письма (накладной) | Откуда поступило, название и год издания | Количество экз. | № экз. | Кому отправлено, дата и исход. № | Кол-во экз. | № экз. | Отметка о переучете или уничтожении |
|-------|---|--|-----------------|--------|----------------------------------|-------------|--------|-------------------------------------|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |

ДОГОВОР №

коллективного подряда на комплексное режимное обслуживание предприятия

Настоящий договор заключен между предприятием _____ в лице директора _____ и коллективом службы безопасности _____ в лице зам. директора — начальника службы безопасности _____ о нижеследующем:

1. Служба безопасности берет на себя выполнение нижеперечисленных работ по обеспечению безопасности и сохранению коммерческой тайны предприятия:
 - 1.1. Круглосуточная охрана предприятия и контроль за соблюдением мер пожарной безопасности.
 - 1.2. Выписка пропусков для сотрудников предприятия.
 - 1.3. Прием командированных, выписка пропусков для них.
 - 1.4. Выписка предписаний для выполнения заданий командируемым сотрудникам и выдача справок о допуске.
 - 1.5. Разработка номенклатуры должностей, подлежащих согласованию с контрольными органами, и оформление допусков.
 - 1.6. Подготовка по представлению директора перечня сведений, составляющих коммерческую тайну, приказов, инструкций о сохранении коммерческой тайны предприятия.
 - 1.7. Оказание услуг по передаче корреспонденции по телетайпу, телексу, телефаксу и другим системам связи.
 - 1.8. Прием, учет и рассылка открытой корреспонденции.
2. Директор предприятия обязуется:
 - 2.1. За работы, перечисленные в настоящем договоре,

- производить оплату из своих фондов по ведомости на работников службы безопасности в размере _____ рублей ежемесячно.
- 2.2. Принимать работы по акту, утвержденному директором и зам. директора — начальником службы безопасности.
 - 2.3. Обязать сотрудников предприятия выполнять все режимные требования, предусмотренные инструкцией по обеспечению сохранения коммерческой тайны.
 - 2.4. При определении грифа документов руководство ограничительными перечнями сведений, обязательными для исполнителей.
 - 2.5. Немедленно представлять в службу безопасности сведения о вступлении в связь с инофирмами.
3. Настоящий договор заключается на календарный год, с 01.01.20 г. до 31.12.20г., готовится в 2-х экземплярах, каждый экземпляр хранится у директора и в службе безопасности.

Директор предприятия

Зам. директора — начальник службы безопасности

« ____ » _____ 200 г.

« ____ » _____ 200 г.

АКТ
о выполнении работ по Договору № _____

« ____ » _____ 20 ____ г.

Комиссия в составе представителя предприятия в лице его директора _____ и представителя коллектива безопасности в лице зам. директора — начальника службы безопасности провели работу по установлению фактического выполнения коллективом службы безопасности договора № _____ коллективного подряда на комплексное режимное обслуживание _____ за _____ 20 ____ г.

В результате проверки комиссия установила, что все работы по договору в _____ 20 ____ г. Выполнены качественно, в полном объеме и в установленные сроки.

К акту прилагается ведомость на выплату.

Директор предприятия

«__» _____ 200 г.

Зам. директора — начальник
службы безопасности

«__» _____ 200 г.

Приложение 8

КАТАЛОГ обобщенных мероприятий по защите конфиденциальной информации

В каталоге рассматриваются обобщенные мероприятия по защите конфиденциальной информации от разглашения, утечки по техническим каналам и от несанкционированного доступа со стороны злоумышленников, конкурентов и иных субъектов противоправных интересов.

Каталог состоит из трех разделов:

1. Мероприятия по предупреждению разглашения конфиденциальной информации.
2. Мероприятия по защите информации от утечки по техническим каналам.
3. Мероприятия по пресечению несанкционированного доступа к конфиденциальной информации.

Мероприятия по предупреждению разглашения конфиденциальной информации

РАЗГЛАШЕНИЕ — умышленные или неосторожные действия должностных лиц и граждан, приводящие к оглашению конфиденциальной информации, доверенной им по службе, и ознакомлению с ней лиц, не имеющих на это права.

РАЗГЛАШЕНИЕ выражается в сообщении, передаче, предоставлении, пересылке, опубликовании, утере и других способах и реализуется по каналам распространения и средствам массовой информации.

ПРЕДУПРЕЖДЕНИЕ РАЗГЛАШЕНИЯ — это комплекс мероприятий, исключающих или ослабляющих возможность неконтролируемого оглашения конфиденциальной информации.

| № п/п | Способы разглашения | Особенности | ДЕЙСТВИЯ | | |
|-------|---|---|---|--|--|
| | | | Организационные | Организационно - технические | Технические |
| | | | <p>Общеорганизационные меры:</p> <p>1. Перечень сведений, составляющих коммерческую тайну</p> <p>2. Обязательства сотрудников о неразглашении коммерческих секретов</p> <p>3. Мониторинг за лояльностью сотрудников</p> <p>4. Меры ответственности за разглашение конфиденциальной информации</p> <p>5. Охрана зданий, помещений и мест хранения документов</p> | | <p>1. Автоматизированные системы мониторинга за лояльностью сотрудников</p> <p>1. Комплексные системы охраны и режима</p> |
| 1. | Открытое оставление конфиденциальных документов | <p>1. На рабочем столе</p> <p>2. На экране ПЭВМ и в средствах коллективного пользования</p> | 1. Расположение рабочего места, исключающее или ограничивающее возможность наблюдения за документами | 1. Использование штор, занавесок, драпировок | <p>1. Возможный контроль за служебными помещениями с помощью телевизионных систем</p> <p>1. Использование программных средств гашения информации по регламенту</p> |

| | | | | | |
|----|--------------------------------------|--|--|--|--|
| | | 3. В квартире 4. В автомашине | 1. Запрет на работу с конфиденциальной информацией дома 1. Строгий контроль за перевозкой документов. | | |
| 2. | Передачи конфиденциальной информации | 1. По каналам электросвязи 2. При разработке и обработке документов | 1. Использование мер сокрытия содержания передаваемых сведений 2. Сокращение времени передачи информации 3. Использование методов скрытного ведения сеансов связи 1. Разработка документов в специальных тетрадах и блокнотах | 1. Использование технических средств защиты информации 2. Использование маскираторов, скремблеров, средств шифрования и электронной подписи в системах связи и телекоммуникации 1. Разработка документов на ПЭВМ с соблюдением требований защиты конфиденциальной информации | 1. Передача сообщений по защищенным системам связи и телекоммуникации |
| 3. | Сообщение, оглашение | 1. На деловых встречах (переговорах) | 1. Четкая регламентация тематики переговоров. | 1. Запись (аудио или аудио/видео) переговоров с целью последующего анализа их конфиденциальности | 1. Использование замкнутых систем ведения конфиденциальных переговоров |

| | | | | | |
|----|-----------|--|--|---|---|
| | | <p>2. При деловой переписке</p> <p>3. На семинарах, симпозиумах, в печати и других средствах массовой информации</p> <p>4. На выставках, реклама</p> | <p>2. Проведение переговоров в специальных помещениях</p> <p>3. Ограничение на запись информации участниками переговоров: — спец. блокноты — тетради и др.</p> <p>1. Контроль содержания переписки</p> <p>1. Соблюдение требований конфиденциальности</p> <p>1. Тщательный анализ и отбор информационных материалов и демонстрационных изделий 2 Строгий инструктаж сотрудников в целях соблюдения режима конфиденциальности</p> | <p>1. Шифрование текста документов</p> <p>2. Применение устройств скрытного фиксирования незаконного доступа к документам</p> | <p>1. Использование технических средств шифрования документов</p> |
| 4. | Пересылка | 1 По каналам почтовой связи | 1 Шифрование документов | 1 Использование аппаратуры шифрования документов | 1 Использование технических средств шифрования документов |

| | | | | | |
|----|----------------|---|---|---|--|
| | | | <p>2 Применение специальных конвертов, исключающих проникновение к документам</p> <p>3 Опечатывание конвертов и упаковок</p> <p>4 Пересылка спецсвязью или курьерами</p> <p>5 Предварительное оповещение адресата о высылке документов</p> <p>6 Уведомление адресата об ответственности за разглашение конфиденциальных сведений</p> <p>7 Нарочным (знакомый, попутчик)</p> | | |
| 5. | Опубликование | <p>1 В печати, диссертационных исследованиях, на радио, телевидении</p> | <p>1 Предварительный контроль публикуемых материалов</p> <p>2 Перечень сведений, разрешенных к опубликованию в открытой печати</p> | | |
| 6. | Личное общение | <p>1 На встречах</p> <p>2 При телефонных переговорах</p> | <p>1 Соблюдение требований о неразглашении конфиденциальной информации</p> <p>1 Запрещение ведения частных переговоров по служебным телефонам</p> | <p>1 Запись переговоров по служебным телефонам на магнитофон</p> <p>2 Использование аппаратуры закрытия те-</p> | <p>1 Мониторинг телефонных переговоров специальными системами контроля</p> |

| | | | | | |
|----|--------------------------------------|--|---|----------------------|--|
| | | | | лефонных переговоров | |
| 7. | Утеря, утрата документов | <p>1 На работе</p> <p>2 За пределами работы</p> | <p>1 Строгий учет и контроль за разработкой, использованием, хранением документов конфиденциального характера</p> <p>2 Службное расследование</p> <p>1 Запрет на вынос служебных документов за пределы организации без надлежащих мер по защите</p> <p>2 Службное расследование</p> | | |
| 8. | Бесконтрольная разработка документов | <p>1 Необоснованное изготовление документов</p> <p>2 Включение в объемные документы сведений конфиденциального характера</p> | <p>1 Регламентация состава конфиденциальных документов</p> <p>1 Контроль за содержанием документов</p> <p>2 Контроль за степенью секретности документов</p> | | <p>1 Программный контроль изготовления документов на ПЭВМ</p> <p>1 Программный контроль за содержанием документов</p> <p>1 Программный контроль секретности документов</p> |

| | | | | | |
|-----|--|--|---|--|--|
| 9. | Бесконтрольный документооборот | <p>1 Необоснованная рассылка документов</p> <p>2 Необоснованное ознакомление с конфиденциальными документами сотрудников</p> | <p>1 Контроль размножения и рассылки документов</p> <p>1 Контроль ознакомления сотрудников с конфиденциальными документами с учетом системы разграничения допуска</p> <p>2 Контроль передачи документов исполнителям</p> <p>3 Контроль за порядком работы с конфиденциальными документами</p> | | <p>1 Программный контроль изготовления и рассылки документов почтой, средствами телекоммуникации и электронной почты</p> <p>1 Программный контроль допуска сотрудников к конфиденциальной информации</p> <p>1 Контроль исполнения документов</p> |
| 10. | Бесконтрольное хранение и уничтожение документов | | <p>1 Обеспечение сохранности документов</p> <p>2 Своевременное уничтожение документов</p> | 1 Использование технических средств механического уничтожения документов | 1 Своевременное программное уничтожение документов на ПЭВМ |
| 11. | Бесконтрольный прием поступающей корреспонденции | | <p>1 Строгий учет поступающих документов</p> <p>2 Своевременное доведение поступивших документов до руководства и исполнителей</p> | | |

Мероприятия по защите информации от утечки по техническим каналам

УТЕЧКА — это бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена в установленном порядке.

УТЕЧКА возможна по различным техническим каналам утечки информации, в частности по визуаль но-оптическим, акустическим, электронным и материально -вещественным.

ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ — это комплекс мероприятий, исключающих образование технических каналов утечки конфиденциальной информации.

| № п/п | Способы (каналы) | Особенности | ДЕЙСТВИЯ | | |
|-------|----------------------|--|--|---|---|
| | | | Организационные | Организационно-технические | Технические |
| 1. | Визуально-оптические | 1 При обычном освещении и в сложных условиях (сумерки, ночь) | 1 Расширение зоны безопасности 2 Контроль возможности установления наблюдения 3 Использование особенностей местности | 1 Использование защитных средств (шторы, защитные пленки, специальные стекла) 2 Использование средств маскировки | 1 Снижение заметности объектов на фоне местности 2 Активное противодействие наблюдению |
| 2. | Акустические | 1 Прямое распространение звука в закрытых объемах | 1 Ведение конфиденциальных переговоров в специальных защищенных помещениях | 1 Оборудование помещений средствами защиты переговоров от утечки информации по акустическим каналам | 1 Использование защищенных технических средств для ведения конфиденциальных переговоров |

| | | | | | |
|----|------------------|---|--|---|---|
| | | <p>2 Прямое распространение звука на открытом пространстве</p> <p>3 Распространение звука в жестких средах (структурный звук)</p> | <p>1 Ограничение ведения конфиденциальных переговоров на открытом пространстве</p> <p>2 Использование местных предметов и условий при ведении конфиденциальных переговоров</p> <p>1 Выявление возможности образования каналов утечки информации в жестких средах (стены, воздуховоды, коммуникации)</p> | <p>1 Строительно-конструкционные меры, исключающие возможность образования акустических каналов</p> | <p>1 Использование технических средств подавления акустических каналов</p> |
| 3. | Электромагнитные | <p>1 За счет микрофонного эффекта в технических средствах</p> <p>2 За счет магнитной составляющей электромагнитного поля</p> <p>3 За счет паразитной генерации усилителей</p> | <p>1 Принятие мер, исключающих возможность образования канала утечки информации за счет микрофонного эффекта</p> <p>2 Обеспечение контролируемой зоны безопасности</p> <p>1 Обеспечение контролируемой зоны безопасности</p> <p>1 Контроль наличия паразитной генерации усилителей различного назначения в выделенных помещениях</p> | <p>1 Установка аппаратных средств защиты от утечки информации за счет микрофонного эффекта</p> <p>1 Экранирование аппаратуры и помещений</p> <p>2 Заземление аппаратуры</p> <p>1 Экранирование и заземление технических средств и помещений</p> | <p>1 Использование технических средств, не имеющих микрофонного эффекта</p> <p>1 Использование защищенных технических средств</p> |

| | | | | | |
|----|--------------------------|--|---|---|---|
| | | <p>4 По цепям питания электронных систем</p> <p>5 По цепям заземления</p> <p>6 За счет взаимного влияния проводов и линий связи</p> <p>7 За счет высокочастотного навязывания</p> <p>8 По волоконно-оптическим каналам связи</p> | <p>1 Использование сетей питания, не имеющих выхода за пределы контролируемой зоны</p> <p>1 Обязательное использование самостоятельных контуров заземления для выделенных помещений</p> <p>1 Исключить параллельный пробег телефонных проводов и линий связи, по которым ведется передача конфиденциальной информации</p> <p>1 Исследование возможностей образования каналов утечки информации за счет ВЧ-навязывания</p> <p>1 Контроль возможного образования каналов утечки по волоконно-оптическим каналам</p> | <p>1 Разборка электрических цепей</p> <p>1 Регулярное измерение сопротивления заземления на соответствие нормативным требованиям</p> <p>1 Использование экранированных кабелей</p> <p>2 Использование различных приемов прокладки проводов, ослабляющих взаимное влияние</p> <p>1 Строгое соблюдение требований по соблюдению мер защиты от утечки информации</p> | <p>1 Использование сетевых фильтров</p> <p>1 Использование отдельного контура заземления</p> |
| 4. | Материально-вещественные | 1 Бесконтрольный выход продуктов отхода производства за пределы территории предприятия | 1 Строгий контроль и ограничение (исключение) выхода продуктов отхода производства за пределы территории предприятия | <p>1 Исключение отходов в качестве вторичного сырья</p> <p>2 Утилизация отходов</p> | <p>1 Системы безотходного производства</p> <p>2 Система очистки жидких и газообразных веществ</p> |

| | | | |
|--|--|---|---|
| | 2 Бесконтрольный выход отходов информационных технологий за пределы территории предприятия | 1 Организация уничтожения информации на технических носителях | 1 Установки уничтожения информации на неисправных носителях |
|--|--|---|---|

Мероприятия по пресечению несанкционированного доступа к конфиденциальной информации

НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП к источникам конфиденциальной информации — это противоправное преднамеренное овладение охраняемыми сведениями лицом, не имеющим права доступа к ним.

НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП (НСД) реализуется различными способами посредством каналов проникновения на объекты криминальных интересов.

ПРЕСЕЧЕНИЕ несанкционированного доступа — это комплекс мероприятий, исключающих или ослабляющих возможность проникновения к коммерческим секретам заходowymi и безза-ходowymi способами.

| № п/п | Способ несанкционированного доступа | Особенности | ПРОТИВОДЕЙСТВИЕ | | |
|-------|-------------------------------------|--|---|---|------------------|
| | | | Организационные меры | Организационно-технические меры | Технические меры |
| 1. | Инициативное сотрудничество | 1 Условия, провоцирующие инициативное сотрудничество | 1 Исключение условий, способствующих инициативному сотрудничеству 2 Анализ и контроль социальных условий в трудовых коллективах 3 Изучение сотрудников, потенциально способных к инициативному сотрудничеству | 1 Использование технических средств контроля социально-морального климата | |

| | | | | | |
|----|----------------------------|---|---|--|---|
| 2. | Склонение к сотрудничеству | 1 Шантаж, запугивание, подкуп | 1 Изучение сотрудников, представляющих интерес для конкурентов и преступных групп | | |
| 3. | Выпытывание, выведывание | 1 Провоцирование на разговоры сотрудников на служебные темы на работе, в общественных местах, на отдыхе и др 2 Выведывание при ведении телефонных разговоров | 1 Обучение и воспитание кадров в направлении строгого соблюдения требований по защите коммерческих секретов | 1 Использование портативных магнитофонов для контроля записей и последующего анализа на предмет выявления злонамеренных действий 1 Использование специальных магнитофонов для записи и анализа злонамеренных действий | 1 Использование аппаратуры контроля телефонных переговоров |
| 4. | Подслушивание | 1 Подслушивание конфиденциальных разговоров руководства и сотрудников в помещениях 2 Подслушивание конфиденциальных переговоров в автотранспорте | 1 Ведение конфиденциальных разговоров в специальных помещениях 1 Запрет на ведение конфиденциальных переговоров в автотранспорте | 1 Оборудование помещений шумопоглощающими средствами 2 Постановка акустических помех 1 Использование средств постановки акустических помех | 1 Использование специальных систем ведения конфиденциальных бесед (переговоров) |

| | | | | | |
|----|-----------------------|--|---|------------------------------------|-------------------------------|
| | | 3 Подслушивание конфиденциальных разговоров на открытой местности | 1 Информирование сотрудников о возможности использования злоумышленниками направленных микрофонов 2 Ведение переговоров с использованием маскирующих свойств местности | | |
| 5. | Визуальное наблюдение | 1 Использование злоумышленником визуальных средств наблюдения за состоянием и деятельностью предприятия (организации) 2 Использование злоумышленником оптических средств наблюдения | 1 Использование штор, занавесей, драпировок | 1 Использование специальных стекол | 1 Постановка оптических помех |
| 6. | Хищение | 1 Первичных документов | 1 Строгий учет и контроль разработки движения и уничтожения документов | | |

| | | | | | |
|----|------------------------|---|--|--|--|
| | | <p>2 Носителей конфиденциальной информации</p> <p>3 Промежуточных документов</p> <p>4 Исходящих документов</p> <p>5 Производствен-ных отходов</p> | <p>1 Строгая регламентация правил сбора и уничтожения отходов</p> | <p>1 Строгий учет и контроль движения технических носителей информации организационно-техническими мерами</p> <p>1 Установка специальных ящиков для отходов производства</p> | <p>1 Широкое использование программных методов обеспечения защиты информации</p> <p>1 Использование аппаратуры и оборудования для уничтожения отходов производства</p> |
| 7. | Копирование | 1 Копирование | <p>1 Регламентация и учет разработки, размножения и рассылки конфиденциальных документов</p> <p>2 Копирование данных и программ на ЭВМ</p> | <p>1 Строгая регламентация технологий обработки информации</p> <p>2 Учет и регистрация режимов работы и выдачи документов</p> | <p>1 Использование программной защиты от несанкционированных действий с конфиденциальной информацией при работе на ПЭВМ</p> |
| 8. | Подделка (модификация) | 1 Подделка деловых документов | 1 Строгий контроль изготовления, учета и рассылки документов | 1 Использование специальных средств подтверждения подлинности документов (специальные чернила и краски и др) | 1 Использование специальной аппаратуры обнаружения исправлений и подделки документов |

| | | | | | |
|-----|--|--|---|--|---|
| | | 2 Подделка финансовых документов 3 Подделка личных документов | 1 Использование специальных методов изготовления личных документов | | |
| 9. | Уничтожение (порча, разрушение) | 1 Документов 2 Продукции 3 Программного обеспечения | 1 Исключение несанкционированного доступа к конфиденциальным документам 1 Обеспечение мер по охране и защите продукции в местах ее нахождения 1 Обеспечение мер по разграничению доступа к программному обеспечению | 1 Использование специальных сейфов для хранения конфиденциальных документов 1 Использование программно-аппаратных методов защиты программ и массивов данных от неправомерного воздействия | 1 Использование охранно-пожарных систем наблюдения и контроля |
| 10. | Незаконное подключение к линиям и системам связи | 1 Контактное | 1 Использование скрытых коммуникаций 2 Охрана мест возможного подключения | 1 Контроль линий и систем связи на наличие подключений 2 Использование экранированных кабелей | 1 Использование средств противодействия незаконному подключению (заземление, прожигание) 2 Использование средств маскирования или шифрования передаваемой информации |

| | | | | | |
|-----|------------------------|---|--|---|---|
| | | 2 Бесконтактное | 1 Использование скрытых коммуникаций 2. Охрана мест возможного подключения | 1 Использование экранированных кабелей | 1 Использование средств маскирования или шифрования передаваемой информации |
| 11. | Перехват | 1 Перехват информации, передаваемой по системам радиосвязи 2 Перехват информации за счет ПЭМИН | 1 Использование методов скрытного ведения сеансов связи 2 Запрещение ведения переговоров конфиденциального характера 1 Проведение мероприятий по исключению образования ПЭМИ | 1 Использование технических средств засекречивания информации 1 Использование способов ослабления ПЭМИН 2 Экранирование помещений | 1 Использование защищенных средств связи 1 Использование активных мер подавления ПЭМИН |
| 12. | Негласное ознакомление | 1 С документами 2 С информацией на экранах ПЭВМ | 1 Организация работы с документами, исключающая возможность ознакомления с их содержанием | | |
| 13. | Фотографирование | 1 Документов 2 Продукции | 1 Организация работы с документами, исключающая возможность ознакомления с их содержанием | | |

| | | | | | |
|-----|--------------------------------|--|--|--|--|
| 14. | Сбор и аналитическая обработка | | 1 Разработка системы мер по сокрытию конфиденциальной информации 2 Четко организованная работа по дезинформированию злоумышленников | | |
|-----|--------------------------------|--|--|--|--|

Список литературы

Официальные документы:

Венская конвенция ООН «О договорах международной купли-продажи товаров», 11.04.80.

Мадридское соглашение «О международной регистрации товарных знаков», 14.04.91.

Парижская конвенция «Об охране промышленной собственности», 20.03.83.

Федеральный закон РФ № 5485-1 «О государственной тайне», 21.07.93.

Федеральный закон РФ № 131-ФЗ «О внесении изменений и дополнений в Закон РФ «О государственной тайне», 6.10.97.

Федеральный закон РФ «О международных договорах РФ», 16.07.95.

Федеральный закон «Об участии в международном информационном обмене», 05.07.96.

Федеральный закон РФ «Об информации, информатизации и защите информации», 25.01.95.

Закон «О предприятиях и ограничении монополистической деятельности на товарных рынках», 21.03.91.

Закон «Об иностранных инвестициях в РФ», 04.07.91.

Указ Президента РФ № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации», 3.04.95.

Указ Президента № 21 «О мерах по упорядочению разработки, производства, реализации, приобретения в целях продажи, ввоза в РФ и вывоза за ее пределы, а также использования специальных технических средств, предназначенных для негласного получения информации», 09.01.96.

Указ Президента РФ №188 «Об утверждении перечня сведений конфиденциального характера», 06.03.98.

Указ Президента РФ № 61 «О перечне сведений, отнесенных к государственной тайне», 24.01.98.

Постановление Правительства РФ № 973 «Об утверждении Положения о подготовке к передаче сведений, составляющих государственную тайну, другим государствам», 02.08.98.

Постановление Правительства РФ № 564 «Об утверждении

Положения о лицензировании деятельности по международному информационному обмену», 03.06.98.

Распоряжение Правительства РФ «О мероприятиях по совершенствованию системы создания и защиты научно-технологических достижений и механизмов их использования в РФ», № 540-р, 20.04.95.

«Положение о порядке контроля за вывозом из РФ товаров и технологий двойного назначения, экспорт которых контролируется», № 1172,07.10.96.

Государственная техническая комиссия при президенте Российской Федерации специальные требования и рекомендации по технической защите конфиденциальной информации.

Руководящий документ Гостехкомиссии России «Защита от НСД к информации. Термины и определения».

Проект федерального закона РФ «О праве на информацию».

Извлечения из проекта закона РФ «О национальной безопасности».

Специальная литература:

Аналитический отчет фирмы «Информационная индустрия», «Индустрия информации сегодня» // Человек и закон: Спецвыпуск.— 1995.

Апполонский СМ. Справочник по расчету электромагнитных экранов.— Л.: Энергоатомиздат, 1988.

Бадалов А.Л., Михайлов А.С. Нормы на параметры электромагнитной совместимости РЭС.— М.: Радио и связь, 1986.

Бизнес и безопасность в России // Человек и закон.— 1996.

Билько М.Н., Томашевский А.К. Измерения мощности на СВЧ.— М.: Радио и связь, 1986.

Буга Н.Н., Конторович В.Я., Носов В.И. Электромагнитная совместимость РЭС.— М.: Радио и связь, 1993.

Вартансян В.А. Радиоэлектронная разведка.— М.: Воениздат, 1991.

Виницкий А.С. Автономные радиосистемы: Учебное пособие для вузов.— М.: Радио и связь, 1986.

Высоцкий Б.Ф. Введение в специальность конструктора РЭС.— М.: Высшая школа, 1990.

Внешнеэкономический бизнес в России: Справочник / Под ред. И.П. Фаминского.— М.: Республика, 1997.

Гавриш В.А. Практическое пособие по защите коммерческой

тайны.— Симферополь: Таврия, 1994.

Гасанов Р.М. Шпионаж особого рода.— М.: Мысль, 1989.

Гонда С, СэкоД. Оптоэлектроника в вопросах и ответах.— М.: Экономика, 1991.

Граднев И.Н., Верник СМ. Линии связи: Учебник для вузов.— М.: Радио и связь, 1988.

Демин А.И. Информационная теория экономики.— М.: Палев, 1996.

Джеэволд У. С. Секреты заключения международных сделок.— М., 1991.

Информационно-коммерческая безопасность: защита коммерческой тайны.— СПб.: Безопасность бизнеса, 1993.

Зиновьев А.Л., Филиппов Л.Н. Введение в специальность радиоинженера.— М.: Высшая школа, 1989.

Калинин А.А., Черепкова Е.А. Распространение радиоволн и работа радиолиний.— М.: Радиосвязь, 1963.

Кащеев В.И. Мониторинг телефонной сети // Системы безопасности.— 1995.— № 1.— С. 51.

Кащеев В.И. Обеспечение информационной безопасности коммерческого объекта // Системы безопасности.— 1995.— октябрь—ноябрь.

Козлов СБ., Иванов Е.В. Предпринимательство и безопасность.— М.: Универсум, 1991.— Т. 1,2.

Крысий А.В. Безопасность предпринимательской деятельности.— М.: Финансы и статистика, 1996.

Куваева М.В., Чуфаровский Ю.В., Шиверский АЛ. Коммерческая информация: способы получения и защиты.— М.: Юрист, 1996.

Курбатов В.И. Стратегия делового успеха.— Ростов-н/Д, 1995.

Лебедев М.М. Уметь вести переговоры.— М.: АНКЛ, 1991.

Леонов С.Л. Радиолокационные средства ПВО.— М.: Воениздат, 1988.

Ллойд К.Ф. Телефонный разговор с клиентом.— М., 1994.

Мазеркин Д. Защита коммерческой тайны на предприятиях различных форм собственности // Частный сыск и охрана.— 1994.

Милич П. Как проводить деловые беседы.— М., 1987.

Мухамедшин И.С. Коммерческая реализация, приобретение и правовая защита технологий // Экономика внешних связей России.— М.: БЕК, 1995.

О концепции правового обеспечения информатизации

России / Бачило Н.А., Белов Г.В., Копылов В.А. и др. // Труды Института законодательства и сравнительного правоведения при ВС РФ.— № 52.— 1992.—С. 4-17.

Оптическая электроника / Василевский А.М. и др.— Л.: Энергоатомиздат, 1990.

Орлов В.А., Петров В.И. Приборы наблюдения ночью и при ограниченной видимости.— М.: Воениздат, 1989.

Палий А.Н. Радиоэлектронная борьба.— М.: Воениздат, 1989.

Поляков В.Т. Посвящение в радиоэлектронику.— М.: Радио и связь, 1988.

Полянский Э. Формула безопасности.— М.: Юридическая литература, 1991.

Предприниматель в опасности: способы защиты / Казакевич О.Ю., Кочев Н.В., Максименко В.Г., Пи-пия А.Г., Шифн Н.И. / УППИКС— М., 1992.

Руководство по организации защиты коммерческой тайны / Под ред. А.Ф.Мохова.— М.: Минатомэнер-го, 1991.

Самойлов В. Система безопасности предприятия // Мы и безопасность.— 1996.— № 2.— С. 19-20.

Сборник материалов по предпринимательству и внешне-неэкономической деятельности. Коммерческие условия внешнеторговых сделок.— М.: РОСБИ, 1996.

Системы радиосвязи: Учебное пособие для вузов.— М.: Радио и связь, 1988.

Съем информации по виброакустическому каналу // Системы безопасности.— 1995.— октябрь —ноябрь.— С. 56.

Подслушивание телефонных переговоров и меры борьбы с подслушиванием // Телефония и телеграфия: Учебник академии связи. —Л., 1961.— С. 328 — 343.

Уокер Ф. Электронные системы охраны.— М.: За и против, 1991.

Халяпин Д.Б., Ярочкин В.И. Основы защиты информации.— М.: ИПКИР, 1994.

Шиверский А.А. Защита информации: проблемы теории и практика.— М.: Юрист, 1996.

Цыкин Т.С. Усилители электрических сигналов.— М.: Энергоатомиздат, 1988.

Экономическая безопасность предприятия: защита коммерческой тайны.— М.: Аналитик-пресса, 1991.

Эрнст О. Слово предоставлено Вам. Практические рекомендации по ведению деловых бесед и переговоров.— М.:

Экономика, 1988.

Янг С, Эллисон А. Измерение шума машин.— М.: Энергоатомиздат, 1988.

Ярочкин В.И. Безопасность информационных систем.— М.: Ось-89, 1996.

Ярочкин В. И. Инструкция по защите конфиденциальной информации при работе с зарубежными партнерами.— М.: ИПКИР, 1998.

Ярочкин В.И. Несанкционированный доступ к источникам конфиденциальной информации // Ярочкин В.И. Предприниматель и безопасность.— М.: Ось-89, 1994.

Ярочкин В.И. Обеспечение сохранения коммерческой тайны предприятия.— М.: ИПКИР, 1998.

Ярочкин В.И. Технические каналы утечки информации.— М.: ИПКИР, 1994.

Ярочкин В.И., Шевцова Г.Л. Каталог обобщенных мероприятий по защите конфиденциальной информации.— М.: ИПКИР, 1997.

Периодические издания:

Иностранец.— 1995.— № 3-17; 1996.— № 1-14.

Журнал официальной информации КАДАСТР.— 1995.— № 35.— сентябрь.— С. 57; 1996.— № 41.— ноябрь.— С. 15-28.

Научная информация.— 1996.— № 19.

Финансовая газета.— 1996.— № 18.— С. 7.

Владимир Иванович Ярочкин

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Компьютерная верстка А. С. Шужин Корректор Ю. В. Рудык

ООО «Академический Проект» Изд лиц № 04050 от 20 02 01
111399, Москва, ул. Мартеновская, 3, стр. 4 Санитарно-
эпидемиологическое заключение Департамента
государственного эпидемиологического надзора № 77 99 02 953
Д 0086 63 11 03 от 28 11 2003 г

ООО «Гаудеамус» 115162, Москва, ул. Шухова, д 21

*По вопросам приобретения книги просим обращаться
в ООО «Трикта»*

111399, Москва, ул. Мартеновская, 3, стр. 4

Тел.: (095) 305 3702; факс: 305 6088

E-mail: aproject@ropnet.ru

[www. aproject.ru](http://www.aproject.ru)

Налоговая льгота — общероссийский классификатор продукции
ОК-005-093, том 2, 953000 — книги, брошюры

Подписано в печать 10.02.2004. Формат 84х108/32. Гарнитура
Балтика. Печать офсетная. Усл.-печ. л. 28,56. Тираж 3000 экз. Заказ
№ 877.

Отпечатано в полном соответствии
с качеством предоставленных диапозитивов
в ОАО «Дом печати — ВЯТКА»
610033, г. Киров, ул. Московская, 122.

В. И. Ярочкин

Информационная безопасность



Ярочкин Владимир Иванович

Кандидат военных наук, доцент по кафедре противодействия иностранным техническим разведкам, профессор Академии военных наук, член-корреспондент Российской академии естественных наук и Международной академии энергоинформационных наук, автор свыше 120 печатных работ, в том числе семи монографий, среди которых наиболее значимые: «Секьюритология», «Недобросовестная конкуренция», «Безопасность информационных систем» и др.

ISBN 5 98426-008-5



9 785984 260084