

Болдырев А. И.  
Василевский И. В.  
Сталенков С. Е.

**Методические рекомендации  
по поиску и нейтрализации средств  
негласного съема информации**

**ПРАКТИЧЕСКОЕ  
ПОСОБИЕ**



---

Болдырев А.И.  
асилевский И. В.  
Сталенков С. Е.

*МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ  
ПО ПОИСКУ И НЕЙТРАЛИЗАЦИИ  
СРЕДСТВ НЕГЛАСНОГО СЪЁМА  
ИНФОРМАЦИИ*

Москва 2001г.

Все права по изданию и распространению на территории РФ и за рубежом принадлежат ЗАО НПЦ Фирма "НЕЛК". Перепечатка издания или его части без разрешения владельцев авторских прав запрещена.

**Авторы:** Болдырев А.И.  
Василевский И.В.  
Сталенков СЕ.  
**художник:** Болдырева И.Б.

В работе изложены современные взгляды на организацию проведения поисковых работ с целью пресечения утечки информации через внедряемые противником скрытые видеокамеры, подслушивающие устройства и другие средства негласного съёма конфиденциальной информации. Работа написана на основе открытых материалов, опубликованных в отечественной и иностранной специальной литературе, периодических изданиях, а также опыта проведения комплексных специальных проверок помещений специалистами НПЦ Фирма «НЕЛК».

Для руководителей и специалистов служб безопасности и подразделений по защите информации, а также интересующихся вопросами защиты информации руководителей фирм организаций.

---

## Содержание

Введение.....	5
1. Подготовительный этап проведения комплексных специальных проверок помещений.....	10
1.1. Уточнение перечня охраняемых сведений и степени важности защищаемой информации .....	13
1.2. Определение вероятного противника и тактики его действий.....	15
1.3. Разработка замысла проведения специальной проверки помещений.....	19
1.4. Изучение и предварительный осмотр объектов проверки.....	23
1.5. Выбор аппаратуры для проведения проверки, распределение сил и средств.....	26
1.6. Составление плана проведения специальной проверки.....	29
1.7. Предварительный анализ радиоэлектронной обстановки .....	33
1.8. Завершающие работы подготовительного этапа.....	38
2. Этап непосредственного проведения комплексной специальной проверки помещений.....	39
2.1. Визуальный осмотр ограждающих конструкций, мебели и других предметов интерьера помещений .....	41
2.2. Проверка элементов строительных конструкций, мебели и других предметов с использованием специальных технических средств.....	50
2.3. Проверка линий и оборудования проводных коммуникаций.....	55
2.4. Радиомониторинг проверяемых помещений, локализация радиоизлучающих средств негласного съёма информации.....	64
2.5. Поиск средств негласного съёма информации, внедрённых в электронные приборы .....	70

---

3. Заключительный этап комплексной специальной проверки помещений .....	73
3.1. Обработка результатов исследования.....	74
3.2. Определение характеристик изъятых средств негласного съёма информации .....	76
3.3. Составление описания проведённых работ .....	78
3.4. Разработка рекомендаций по повышению защищённости помещений.....	79
3.5. Составление акта проведения комплексной специальной проверки помещений.....	85
3.6. Завершающие работы заключительного этапа.....	85
Заключение.....	88
Приложение 1 .....	89
Словарь основных терминов и определений .....	89
Приложение! .....	91
Классификация технических каналов утечки информации (вариант).....	91
Перечень специального оборудования и технических средств, рекомендуемых для проведения комплексной специальной проверки помещений.....	95
Таблица 2.....	95
Приложение 4 .....	96
Справочные данные по распределению радиочастот.....	96
Приложение 5 .....	102
Формализованный вариант плана проведения комплексной специальной проверки помещений.....	102
Формализованный вариант акта проведения комплексной специальной проверки помещений.....	108
Отчёт, формируемый комплексом КРОНА-6000М (вариант).....	111
Рекомендации по повышению защищённости помещений и объектов (вариант).....	113

## Введение

Развитие в обществе рыночных отношений неминуемо сопровождается обострением конкурентной борьбы между производителями товаров и услуг. При этом всегда находятся отдельные личности и группы людей, готовые применить в конкурентной борьбе методы, отвергаемые цивилизованным миром. К таким методам относятся подкуп должностных лиц, кража чужих технологий и результатов научных исследований, целенаправленная дискредитация конкурентов. Демократическому обществу присущ и такой недостаток, как наличие криминальных элементов и групп, целиком посвятивших себя преступному бизнесу. В их арсенале - вымогательство, основанное на шантаже и угрозах в адрес предпринимателей, бизнесменов, руководителей и должностных лиц деловых, коммерческих и даже государственных структур.

Криминальная деятельность преступных сообществ и недобросовестных конкурентов практически всегда основывается на краже или добывании другими способами информации, позволяющей им спланировать и реализовать свои намерения. Довольно часто кража информации представляет собой не подготовку, а непосредственную цель преступных действий. Обычно это относится к информации, которая позволяет конкурентам заключить выгодный для себя контракт или воспользоваться результатами чужого труда, сэкономив тем самым средства на проведении собственных исследований или приобретении этих результатов законным путём. Поскольку ценная конфиденциальная информация обладает качествами товара, она может добываться в целях последующей продажи заинтересованным лицам и организациям.

Для добывания информации используются различные методы. Они включают хищение носителей информации, её несанкционированное копирование, подслушивание, перехват информативных побочных электромагнитных излучений и наводок, перехват информации, передаваемой по системам связи, и другие противоправные действия. Особое место среди них занимает съём информации с помощью намеренно внедрённых в помещения, подключённых к средствам обработки информации или каналам связи специальных технических средств негласного съёма информации (далее - *средств НОТ*). В общем виде под средством (системой) НСИ мы понимаем специальное техническое средство (систему) или совокупность технических средств, применяемых злоумышленником для преобразования, передачи, приёма (перехвата) и регистрации информативных сигналов с целью получения неправомерного доступа к чужой информации. При этом под информативным сигналом подразумевается любой сигнал (звуковой, зрительный, электромагнитный и др.), содержащий информацию о сведениях,

относимых к защищаемой информации.

Одним из видов или элементом средств (систем) НСИ является *закладочное устройство*, скрытно внедряемое (закладываемое или вносимое) в места возможного съёма информации. Номенклатура таких устройств на сегодняшний день чрезвычайно обширна. Она включает средства перехвата информации с каналов связи, диктофоны, радиомикрофоны, сетевые микрофоны, устройства скрытого видеонаблюдения, стетоскопы, преобразователи (усилители) информативных сигналов и другие технические средства. Современные закладочные устройства, как правило, отличаются превосходным качеством маскировки, высокими техническими характеристиками и простотой установки.

Выявление и нейтрализация внедрённых средств НСИ - одно из важных направлений в защите информации на любых предприятиях, в учреждениях и организациях независимо от их организационно-правовой формы собственности. Особое внимание при этом уделяется охране сведений, отнесённых к государственной или служебной тайнам. Защита этих сведений в Российской Федерации осуществляется в рамках государственной системы защиты информации, созданной в соответствии с федеральными законами «О государственной тайне» и «Об информации, информатизации и защите информации». Мы не собираемся раскрывать в деталях работу подразделений, осуществляющих выявление средств НСИ в помещениях органов государственной власти и предприятий, имеющих дело со сведениями, отнесёнными к государственной или служебной тайнам, тем более что часть руководящих нормативно-методических документов для таких подразделений сама относится к информации ограниченного доступа. В данной публикации мы ограничимся вопросами защиты сведений, представляющих собой коммерческую тайну, а также любой другой информации, относимой её собственником к категории защищаемой.

Как известно, под защитой информации понимается деятельность, направленная на предотвращение её утечки, а также несанкционированных и непреднамеренных воздействий на информацию [1]. Причинами утечки информации могут быть её разглашение (неконтролируемое распространение), нарушение заинтересованными лицами установленных правил доступа к защищаемой информации (несанкционированный доступ), а также целенаправленная деятельность разведок, в том числе, с помощью технических средств. В соответствии с [2], использование закладочных устройств, а также подключение к техническим средствам и системам помещений, в которых циркулирует защищаемая информация, относят к несанкционированному доступу к информации. Применение технических средств перехвата электромагнитных излучений, наводки и других средств НСИ, позволяющих реализовать способы дистанционного съёма защищаемой информации без необходимости хотя бы однократного захода в помещение,

где она циркулирует, обычно классифицируют, как ведение разведки с использованием технических средств. Исходя из этого, защиту информации < г г подслушивающих, подглядывающих и других средств НСИ следует относить к мерам противодействия несанкционированному доступу и разведке, ведущейся с применением технических средств.

Применение в данной области терминологии, более присущей ведению боевых действий, не случайно. Для внедрения средств НСИ обычно привлекают наёмников-профессионалов в добывании защищаемой информации. Действиям таких наёмников может противостоять только постоянная целенаправленная работа других профессионалов - специалистов по защите информации. Поэтому борьба со средствами НСИ - это всегда борьба двух коллективных интеллектов, двух враждующих «армий», на вооружении которых состоят последние достижения науки и техники. Действия каждой из сторон в этой бескомпромиссной борьбе сродни военной операции. Из этого следует, что действия по выявлению и нейтрализации средств НСИ, как и всякая военная операция, требуют для своего успеха тщательной подготовки грамотного проведения.

К настоящему времени накоплен достаточно большой опыт организации и проведения поисковых работ по выявлению внедрённых в помещения, предметы, электронные приборы или подключённых к средствам обработки информации, каналам связи средств НСИ. Наиболее полными по объёму и номенклатуре проводимых работ являются комплексные специальные проверки помещений, методике проведения которых и посвящена данная публикация.

*Цель* проведения комплексных специальных проверок помещений заключается в пресечении (предотвращении) получения злоумышленником (противником) защищаемой информации из этих помещений с помощью средств НСИ. Тем самым предотвращается ущерб, который может быть нанесён собственнику, владельцу, пользователю защищаемой информации в случае использования злоумышленником (противником) этой информации в своих интересах.

С технической точки зрения средство НСИ является одним из элементов организованного злоумышленником канала съёма информации, включающего объект разведки (информативный сигнал), техническое средство (систему) разведки (средство НСИ) и физическую среду распространения информативного сигнала. Совокупность этих элементов составляет *технический канал утечки информации* (далее для краткости - ТКУИ) [3].

Объективную возможность организации злоумышленниками различных ТКУИ создаёт многообразие источников опасных, то есть таких, которые потенциально могут быть перехвачены, информативных сигналов, разнообразная физическая природа их образования и распространения в различных физических средах. Одни из возможных вариантов классификации



различных ТКУИ приведён в приложении 2.

ТКУИ, которые при наличии определённых условий и специальных технических средств разведки могут быть организованы злоумышленниками, называют *потенциальными*. В ходе комплексных специальных проверок помещений должны быть выявлены потенциальные ТКУИ и выработаны рекомендации по их закрытию (ликвидации). Кроме того, проведение любой проверки должно способствовать повышению уровня подготовки специалистов по защите информации за счёт накопления и анализа новых данных о возможностях негласного съёма информации.

С учётом этого *основными задачами* комплексных специальных проверок помещений можно считать:

- выявление и нейтрализация внедрённых противником средств НСИ;
- выявление незакрытых потенциальных ТКУИ;
- определение мероприятий, требуемых для закрытия (ликвидации) выявленных потенциальных ТКУИ;
- сбор новых сведений о тактике применения противником средств НСИ их характеристиках.

Многолетний опыт работ в области защиты информации позволяет утверждать, что успеху поисковых мероприятий способствует соблюдение определённых принципов их организации и проведения. *Основными принципами* организации и проведения комплексных специальных проверок помещений следует считать:

- соответствие положениям законов и других правовых актов, регулирующих отношения в области защиты информации (правозаконность);
- скрытность подготовки и выполнения работ;
- системность (периодичность) проведения;
- взаимосвязь с другими мероприятиями в общей системе защиты информации;
- комплексность применяемых методов и технических средств;
- достаточность проводимых работ для достоверной оценки защищённости помещений;
- комплексность разрабатываемых организационных, инженерных и технических мер защиты;
- достаточность рекомендуемых мер защиты для предотвращения утечки информации по выявленным потенциальным ТКУИ.

Комплексные специальные проверки помещений занимают заметное место в общей системе мероприятий по защите информации. Они проводятся при аттестации помещений, периодически (в соответствии с заранее разработанным планом-графиком), после проведения в помещениях каких-либо работ (ремонта, монтажа оборудования, изменения интерьера и т.д.) или неконтролируемого посещения посторонними лицами, а также во всех случаях,

когда возникает подозрение в утечке информации через возможно внедрённые средства НСИ.

Вместе с тем, проведение комплексных специальных проверок помещений не позволяет защитить охраняемые сведения от всех видов угроз.<sup>1</sup> {арубежный и отечественный опыт защиты информации говорит о том, что наиболее эффективной может быть только комплексная защита, сочетающая в себе и правовое, и организационное, и инженерно-техническое направления. С этой точки зрения комплексные специальные проверки помещений можно рассматривать лишь в качестве одного из элементов подсистемы защиты информации от её утечки по техническим каналам в составе комплексной системы защиты информации на предприятии или фирме [4].

Говоря о правовой основе проведения защитно-поисковых мероприятий по выявлению средств НСИ, следует прежде всего иметь в виду, что согласно Федеральному закону «Об информации, информатизации и защите информации», право на установление режима защиты конфиденциальной информации предоставлено собственнику информации. То есть, для информации, собственником которой являетесь вы сами, ваше учреждение или предприятие, степень защиты и номенклатуру защитных мероприятий вы можете выбирать сами. Исходя из этого, действия собственника или владельца защищаемой информации по выявлению внедрённых средств НСИ являются абсолютно законными и правомерными. Правда, следует оговориться, что положения указанного закона распространяются только на документированную информацию.

Вместе с тем, существующими законами и нормативными документами предусматривается лицензирование таких видов деятельности, как контроль защищённости информации ограниченного доступа [5,6]. Из этого следует, что силами службы безопасности своего предприятия или фирмы вы можете проводить у себя любые проверки, если только они не нарушают прав личности работающих у вас сотрудников. В случае отсутствия на вашем предприятии развитой собственной службы безопасности или её недостаточной технической оснащённости, для проведения комплексной специальной проверки помещений следует пригласить стороннюю организацию, которая имеет лицензию на проведение такого рода работ. Такая организация по закону несёт полную юридическую и финансовую ответственность за качество выполнения работ и обеспечение сохранности доверенных им секретов.

Необходимо иметь в виду, что Федеральный закон «Об оперативно-розыскной деятельности» даёт право на применение специальных технических средств НСИ оперативным подразделениям семи различных государственных структур. Если проверка ваших помещений обнаружит внедрённые средства НСИ, и у вас будут основания полагать, что это - средства правоохранительных или других органов, осуществляющих оперативно - розыскную деятельность, закон даёт вам право обжаловать их действия в вышестоящий орган, прокурору

или в суд, а также истребовать от органа, осуществляющего оперативно - розыскную деятельность, сведения о полученной о вас с помощью средств НСИ информации.

Использование средств НСИ органами, осуществляющими оперативно - розыскную деятельность, допускается только на основании судебного решения. Несанкционированное применение специальных технических средств НСИ или использование их лицами, не уполномоченными на это Федеральным законом «Об оперативно-розыскной деятельности», преследуется по закону на основании ст. 138 Уголовного кодекса Российской Федерации.

Перечень принятых в работе сокращений:

ИК- инфракрасный;

НСИ - негласный съём информации;

ПЭВМ - персональная электронно-вычислительная машина;

ПЭМИ - побочное электромагнитное излучение;

ТКУИ -технический канал утечки информации.

## 1. Подготовительный этап проведения комплексных специальных проверок помещений.

Зарубежный и отечественный опыт проведения работ по выявлению средств НСИ показывает, что действия по подготовке и проведению комплексных специальных проверок помещений целесообразно условно разделить на **три этапа**: *подготовительный*, *этап непосредственного проведения специальной проверки помещений* и *заключительный* этап.

Работы, составляющие содержание *подготовительного этапа*, представлены на схеме 1.

..... Схема!  
**Подготовительный этап комплексной  
специальной проверки помещений**

---

Уточнение перечня охраняемых сведений и степени важности информации, относимой руководством предприятий (фирмы) к защищаемой.

---

---

Определение вероятного противника, оценка его возможностей, тактики внедрения средств НСИ и их использования.

---

Разработка замысла проведения комплексной специальной проверки помещений:

выработка целевой установки: для противодействия какому противнику следует провести поисковые мероприятия;

определение масштаба и места проведения поисковых мероприятий;

выбор времени проведения проверки;

разработка легенды, под прикрытием которой будет проводится специальная проверка;

выработка замысла активизации активации внедренных средств НСИ;

выработка вариантов действий в случае обнаружения средств НСИ.

Изучение планов помещений, схем технических коммуникаций, связи, организации охраны, доступа и других необходимых документов.

Предварительный осмотр помещений.

Разработка перечня аппаратуры, необходимой для проведения специальной проверки помещений.

Разработка дополнительных мер по активизации внедренных средств НСИ на время проведения поиска с различными типами аппаратуры.

Распределение привлекаемых сил и средств по объектам и видам работ.

Уточнение частных методик использования привлекаемой аппаратуры в конкретных условиях предстоящей проверки.

Оформление плана проведения комплексной специальной проверки помещений и утверждение его у руководителя предприятия.

---

Подготовка аппаратуры для проведения поисковых и исследовательских работ.

---

Предварительный сбор данных и анализ радиоэлектронной обстановки в районе обследуемых помещений.

---

Подготовка документов прикрытия работ по специальной проверке помещений в соответствии с выбранной легендой прикрытия.

---

Подготовка бланков, схем, заготовок других документов, необходимых для проведения работ на последующих этапах.

---

Этот этап является исключительно важным, поскольку качество подготовительных работ предопределяет надёжность результатов проверки. Часть работ этого этапа предполагает участие в них руководителя предприятия, на котором должна быть проведена проверка помещений. Поэтому от того, удастся ли с самого начала достичь взаимопонимания между руководством предприятия специалистами по поисковым работам, в значительной степени зависит эффективность всех поисковых мероприятий.

Следует убедить руководителя предельно ограничить круг лиц, привлекаемых к подготовке проверки, чтобы обеспечить скрытное проведение всех подготовительных работ. Необходимо помнить, что в интересах противника может работать кто-то из сотрудников предприятия. Случайная утечка информации о намечаемой проверке может свести её результативность до нуля. Причиной тому может быть не только возможное изъятие или выключение средств НСИ на период проверки, но и высокая вероятность внедрения таких средств фазу же по окончании проверки, когда руководство и служба безопасности предприятия успокоятся и будут считать помещения «чистыми». Поэтому все согласования вопросов предстоящей проверки целесообразно проводить вне стен предприятия, где-нибудь на нейтральной территории или территории организации, выбранной для проведения специальной проверки помещений.

## 1.1. Уточнение перечня охраняемых сведений и степени важности защищаемой информации.

Тем, кто совершенно чётко представляет себе, какую информацию им нужно защищать от утечки, этот раздел можно не читать. Остальным мы советуем ознакомиться с изложенными здесь рекомендациями, поскольку они помогут вам определить, что и зачем надо защищать. Знание этого повысит вероятность правильного определения противника, намеренного похитить ваши секреты. Незнание противника может привести к недостаточности выбираемых мер защиты или неоправданным затратам на проведение защитных мероприятий.

Суть проблемы в том, что защита информации – довольно дорогое занятие, требующее не только разовых, но и постоянных текущих затрат. Поэтому защищать необходимо только ту информацию, утечка которой может привести к экономическому, моральному или другому ущербу предприятию, организации, её руководству, отдельным сотрудникам предприятия или другим физическим лицам.

Очевидно, что информация, отнесённая к категории защищаемой, может иметь различный характер, и что утечка различной защищаемой информации может привести к разным последствиям. Поэтому необходимо знать не только, что и зачем надо защищать, но и насколько следует защитить конкретный вид охраняемых сведений. Это позволит дифференцировать мероприятия по обеспечению безопасности информации и сократить тем самым затраты на их проведение.

Напомним, что в соответствии с Федеральным законом «Об информации, информатизации и защите информации» степень защиты информации ограниченного доступа определяет её собственник. Ответственность за выполнение мер защиты, установленных собственником информации, закон возлагает не только на собственника, но и на пользователей этой информации. Поэтому важно чётко представлять, какая информация ограниченного доступа, собственником которой вы не являетесь, используется на вашем предприятии, ибо эта информация должна быть защищена вне вашего желания.

Целесообразен следующий порядок действий по определению видов, объёма и степени важности информации, которую вы должны защищать от возможной утечки и других видов угроз:

- Уточняется перечень сведений, которые вы *обязаны защищать* в соответствии с федеральными законами. К ним относятся сведения, составляющие государственную тайну, а также другие сведения, отнесённые их собственниками к категории конфиденциальных. Вы можете быть пользователем или даже владельцем этих сведений, но степень их защиты обязаны обеспечить такую, которую требуют от вас собственники этой

информации. Как уже отмечалось выше, вопросы защиты информации, составляющей государственную тайну, остаются за рамками данной публикации.

• Составляется перечень сведений, являющихся *собственностью вашего предприятия или фирмы*, которые целесообразно отнести к категории защищаемых. Обычно в этот перечень включают:

• сведения, представляющие результаты творческой деятельности и составляющие интеллектуальную собственность вашего предприятия: неопубликованные научно-технические результаты, технические решения, методы, способы использования технологических процессов и устройств, не обеспеченные патентной защитой; сведения об используемых программных продуктах, материалах, элементной базе, комплектующих изделиях и способах производственной продукции, состоянии и особенностях перспективных разработок; содержание коммерческих, методических и организационно-управленческих идей и решений: планов реорганизации, развития и модернизации производства, расширения рынков сбыта товаров и услуг, замыслов очредных рекламных компаний ит. п.; результаты маркетинговых исследований, анализа конъюнктуры рынка, эффективности рекламы, сведения о наиболее выгодных формах использования денежных средств, ценных бумаг, акций ит. п.;

• сведения, составляющие деловую информацию о деятельности предприятия, ваших партнёров и конкурентов: содержание учётных и первичных бухгалтерских документов, промежуточная финансовая информация, деловая переписка, сведения о системе управления предприятия, его кадровом составе, информационные базы данных о клиентах партнёрах, содержание и сам ф акт заключения или предложения о заключении с ними договоров (контрактов), сведения о конкурирующих организациях ит. п.;

■ сведения о системе безопасности предприятия: системах охраны, сигнализации, контроля лояльности сотрудников, применяемых способах и технических средствах защиты информации ит. п.

■ Для каждого из пунктов перечня защищаемых сведений определяется *возможный экономический ущерб* от их утечки, характеризующий собой ценность данной информации. Для оценки возможного ущерба могут быть использованы математические методы или методы экспертных оценок, при этом должны быть учтены как непосредственные, так и косвенные потери. К непосредственным потерям могут быть отнесены, например, возможные финансовые санкции клиентов или ущерб, вызванный утратой информации функций товара из-за её разглашения. К косвенным могут быть отнесены потери из-за подрыва репутации предприятия, снижения банковского доверия, потери клиентуры или её интересов из-за временных задержек, потери вследствие ослабления позиций на рынке и т. п. В большинстве случаев экономический ущерб может быть оценён лишь приблизительно, ибо далеко

не всегда удается предугадать все возможные последствия утечки информации. Максимально объективную оценку возможного ущерба можно получить в случае привлечения компетентных независимых экспертов, способных детально проанализировать все стороны деятельности вашего предприятия.

■ Проводится *ранжирование* (сортировка) пунктов перечня защищаемых сведений *по ценности защищаемой информации*, эквивалентной возможному<sup>7</sup> ущербу от её утечки. В результате этой операции пункты перечня должны быть распределены по нескольким различным группам (категориям), включающим в себя сведения примерно одинаковой ценности.

Выбранное вами количество таких групп (категорий) определит число градаций степени защиты информации в создаваемой вами системе защиты информации. Ценность сведений, включённых в конкретную группу (категорию), позволит обоснованно ограничить номенклатуру защитных мероприятий и средств защиты для каждой группы сведений, дифференцировав и сократив тем самым общие затраты на защиту информации.

Правовую основу охраны сведений, которые вы отнесли к категории защищаемых, призван обеспечить Федеральный закон «О коммерческой тайне», проект которого принят Государственной Думой в начале 1999 года. Чтобы эти сведения попали под охрану закона, перечень сведений, составляющих коммерческую тайну, должен быть утверждён руководителем предприятия и доведён до сотрудников предприятия, допущенных к информации ограниченного доступа и давших письменное согласие на соблюдение установленного режима коммерческой тайны.

При составлении перечня защищаемых сведений следует помнить о том, что постановлением Правительства Российской Федерации от 5 декабря 1991 года № 35 и проектом закона «О коммерческой тайне» определён перечень сведений, которые не могут составлять коммерческую тайну.

## 1.2. Определение вероятного противника и тактики его действий.

Важнейшее место среди работ подготовительного этапа комплексной специальной проверки помещений занимает *выявление или уточнение вероятного противника*, осуществляющего перехват информации с помощью средств НСИ. Конечным результатом работ на этом этапе должно быть составление *модели действий* вероятного противника по добыванию защищаемой информации. Правильное определение противника позволит реально оценить его финансовые, оперативные и технические возможности по номенклатуре применяемых средств НСИ и их характеристикам,



спрогнозировать тактику его действий по установке и внедрению средств НСИ, их практическому использованию. Результаты прогноза противника кладутся в основу замысла проведения поисковых мероприятий, определяют выбор исследовательской и поисковой аппаратуры, тактики действий при обнаружении внедренных средств НСИ и нейтрализации возможных ответных шагов противника.

Ряд существующих организационно-методических документов по защите информации от несанкционированного доступа и технической разведки [7,8] рекомендуют в качестве объекта и нарушителя рассматривать субъекта, имеющего доступ к работе на предприятии, являющегося специалистом высшей квалификации и знающего всё о работе предприятия его системе безопасности, включая полные сведения о системе средств защиты информации. Эти рекомендации можно считать абсолютно правильными, если речь идёт о защите секретов государства от любого вида посягательств, включая действия агентов технической разведки иностранных государств.

Вместе с тем, такой подход к моделированию вероятного противника не всегда оправдан на предприятиях среднего и малого бизнеса, не имеющих дело со сведениями, отнесёнными к государственной тайне. Он может привести к тому, что для отражения угроз, создаваемых таким изолированным противником, понадобится мобилизация всех финансовых и материально-технических ресурсов предприятия.

Мы считаем более целесообразным дифференцированный подход к определению вашего вероятного противника. Многообразие исходных ситуаций для прогнозирования противника, осуществляющего съём вашей информации с помощью средств НСИ, может быть, в принципе, сведено к следующему трём основным.

*Ситуация первая:* вы стремитесь застраховать себя от утечки вполне конкретных сведений, представляющих для вас в настоящее время наибольшую ценность. В этой ситуации следует, по возможности, наиболее полно представить себе в виде перечня, какие организации и частные лица могут быть заинтересованы в получении этих сведений. При составлении перечня «потенциальных противников» не стоит сильно ограничивать себя вашими представлениями о высокой порядочности конкретных организаций, юридических и физических лиц. Реалии современной жизни таковы, что действующим противником может оказаться человек, которому вы всецело доверяли. Поэтому в данном случае лучше переборщить, чем составить неполный список.

Затем следует проанализировать составленный список и попытаться выделить в нём организации и структуры, обладающие наибольшими финансовыми и техническими возможностями. На эти организации следует ориентироваться при составлении модели действий вероятного противника.

*Ситуация вторая:* вы предполагаете или даже точно знаете, утечка

какой защищаемой информации уже нанесла ущерб вашему предприятию или физическим лицам, и хотите пресечь дальнейшую утечку информации по этому канату.

В этой ситуации круг организаций и физических лиц, относимых вами к вероятному противнику, может быть предельно сужен. Прежде всего, необходимо проанализировать, когда, в каком объёме и в какой форме могла произойти утечка этой информации, кем и каким образом она была использована. Это тот самый случай, когда в полной мере может использоваться юридическая формула, восходящая к римскому праву: *сделал тот, кому выгодно.*



*Третья ситуация:* вы собираетесь провести профилактическую специальную проверку помещений, чтобы исключить возможность утечки через средства НСИ любой защищаемой информации. Этот случай можно считать наиболее сложным, ибо он предполагает в качестве вероятного противника не только конкурирующие предприятия, разного рода криминальные элементы и структуры, но и неразборчивых в средствах представителей органов массовой информации, имиджевых и иных фирм, занимающихся сбором компромата по заказу заинтересованных лиц. Вашим противником могут оказаться организации, поддерживающие с вами деловые отношения, отдельные личности. При определении круга ваших вероятных противников следует помнить, что они могут иметь самые разнообразные побудительные мотивы для внедрения на вашем предприятии средств НСИ. Перехват вашей защищаемой информации может, например, проводиться с целью:

- *анализа* вашей деятельности, чтобы проверить вашу кредитоспособность или избежать деловых отношений с возможно недобросовестным партнёром;
- *пресечения* возможно планируемого вами, но невыгодного для себя действия своим упреждающим действием (преднамеренного срыва сделок и иных соглашений);
- последующей *продажи* собранной информации конкурентам, заинтересованным лицам или организациям;
- разглашением собранной информации *заставить* вашего конкурента совершить выгодные для себя действия;
- последующего *шантажирования* вас угрозой разглашения собранной информации, передачи её конкурентам или заинтересованным лицами т.д.

Необходимо учитывать, что в интересах противника может работать кто-либо из работников вашего предприятия. Такой сотрудник может действовать из корыстных побуждений или в отместку руководству предприятия, её отдельным работникам, если он считает себя недооценённым или незаслуженно обиженным. Особую угрозу представляют сотрудники, выполняющие задания конкурирующих предприятий или действующие по заказу криминальных структур. Специалист, выбранный противником для ведения разведки и установки средств НСИ, может быть намеренно внедрён в число работников вашего предприятия. Такой агент может нанести огромный ущерб, особенно, если его удастся внедрить в службу безопасности предприятия. Поэтому на любом предприятии следует иметь систему постоянного контроля лояльности персонала.

Существует также вероятность, что вашим противником является не одна, а сразу несколько организаций, имеющих разные возможности по внедрению средств НСИ. Учитывая возможность координации их действий, при составлении модели вероятного противника и последующем выборе стратегии поиска целесообразно ориентироваться на противодействие организации с более высоким финансово-техническим потенциалом.

Особым случаем можно считать ситуацию, когда в качестве своего вероятного противника вы склонны рассматривать оперативные подразделения правоохранительных и иных государственных структур, имеющих в необходимых случаях практически неограниченные оперативные и технические возможности по съёму интересующей их информации с помощью средств НСИ. Будем, однако, исходить из того, что ваша законопослушная деятельность не даёт повода для особого внимания со стороны таких подразделений.

В подавляющем большинстве случаев определение вероятного противника следует отнести к прерогативе руководителя предприятия, ибо он лучше других представляет себе стратегические задачи предприятия, имеет неограниченный доступ к информации о своих партнёрах, клиентах, конкурентах и сотрудниках и может организовать добывание недостающей информации как гласным, так и негласным путём. В оценке оперативных и технических возможностей вероятного противника по использованию средств НСИ и прогнозировании тактики его действий должны помочь технические специалисты службы безопасности или организации, занимающейся проведением специальных проверок помещений.

Разработанная на этом этапе *модель действий вероятного противника* должна включать:

- мотивы действий вероятного противника или преследуемые им цели;
- наиболее вероятные методы, используемые им для внедрения средств НСИ;

- категорию лиц, к которым могут принадлежать субъекты, выбранные вероятным противником для внедрения средств НСИ и съёма информации;
- возможный уровень знаний, навыков и квалификации субъекта, осуществляющего внедрение средств НСИ;
- техническую оснащённость противника: возможные виды применяемых средств НСИ, их наиболее вероятные потребительские и технические характеристики, способы установки;
  - предполагаемые места, способы и время внедрения средств НСИ;
- действия по съёму информации с внедрённых средств НСИ;
- наиболее вероятные действия в случаях установления противником ваших намерений провести комплексную специальную проверку помещений, факта непосредственного проведения такой проверки факта обнаружения поисковой бригадой внедрённых средств НСИ.

### 1.3. Разработка замысла проведения специальной проверки помещений.

Разработку замысла проведения специальной проверки помещений можно считать наиболее важным элементом работ подготовительного этапа. Замысел, по определению, - это основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели проверки. В состав замысла входят:

- целевая установка: для противодействия какому противнику следует провести поисковые мероприятия;
  - масштаб и место проведения поисковых мероприятий;
  - время проведения проверки;
- легенда, под прикрытием которой будет проводиться специальная проверка;
  - замысел активации внедрённых средств НСИ;
  - варианты действий в случае обнаружения средств НСИ.

Целевая установка непосредственно вытекает из результатов работы по уточнению или выявлению вероятного противника. Результаты оценки финансовых, оперативных и технических возможностей противника определяют и *масштаб проведения* поисковых мероприятий. Под масштабом здесь следует понимать не только количество и общую площадь помещений, которые вы намечаете для специальной проверки, но и глубину поисковых, а также сопутствующих исследований и их номенклатуру. Чем большими финансовыми и техническими возможностями обладает ваш

вероятный противник, тем более тщательными и разносторонними должны быть поисковые работы и работы по исследованию потенциальных ТКУИ. Так, обычно в состав поисковых работ включают визуальный осмотр оборудования, мебели, предметов технологических коммуникаций, проверку элементов строительных конструкций, мебели и других предметов с использованием специальных технических средств, проверку проводных коммуникаций, радиомониторинг проверяемых помещений. В более серьезных случаях дополнительно проводят поиск средств НСИ, внедрённых в электронные приборы, проверку элементов конструкции помещений, трубопроводных и других технологических коммуникаций на наличие в них акустических и виброакустических сигналов из проверяемых помещений, исследование побочных электромагнитных излучений оргтехники и другие исследования.

Выбор *времени проведения* проверки (в рабочий или выходной день, днём или ночью, в рабочее время, до начала рабочего времени или сразу по окончании рабочего дня) непосредственно связан с разработкой *легенды*, под прикрытием которой будет работать поисковая бригада. Выше мы уже говорили о том, что одним из основополагающих принципов проведения комплексных специальных проверок помещений является скрытность выполнения основных работ. Из этого вытекает необходимость разработки для персонала предприятия и посетителей, в том числе, лиц, возможно, работающих на противника, правдоподобной версии (легенды прикрытия) появления на предприятии специалистов, занимающихся проведением измерительных и поисковых работ с использованием сложного и довольно специфического оборудования.

Разработанная легенда прикрытия должна легко вписываться в деятельность предприятия и оказывать минимальное деструктивное влияние на его повседневную деятельность. Весьма вероятно, что придётся разрабатывать не одну, а сразу несколько легенд прикрытия, в том числе, для появления на предприятии одного или нескольких членов поисковой бригады, имеющих задачу провести предварительный осмотр помещений. Для каждой из легенд должны быть разработаны способы и определено время их доведения до персонала предприятия, составлен перечень необходимых для подтверждения легенды оборудования, приборов и документов. Общими требованиями к создаваемым легендам прикрытия являются их правдоподобность, естественность, надёжность и соответствие создаваемой ситуации содержанию работ членов поисковой бригады.

В качестве легенд прикрытия поисковых работ можно рекомендовать:

- проверку специалистами телефонного узла связи состояния телефонных линий и оборудования;
- проверку состояния отопительной системы, водопроводных и других инженерно-технических коммуникаций, проведение на них ремонтных работ;

- плановую проверку функционирования систем охранной пожарной сигнализации;
- проведение регламентных работ на элементах системы внутренней связи предприятия;
  - проверку системы заземления, состояния электроизоляции проводов системы освещения, элементов системы электропитания;
- поиск местонахождения искрящих контактов скрытой электропроводки для устранения помех ПЭВМ;
  - проверку приглашёнными экологами состояния окружающей среды (освещённости рабочих мест, уровня радиации и электромагнитных излучений, состава воздуха и т. п.);
  - подготовку и проведение косметического ремонта помещений.

При выборе времени проведения проверки следует учитывать, что в нерабочее время дистанционно управляемые средства НСИ могут оказаться выключенными. Это заметно снизит вероятность их обнаружения поисковой аппаратурой, поэтому необходимо заранее продумать *меры по активации средств НСИ*. Можно, например, заранее распространить среди сотрудников предприятия информацию о якобы намеченном на выбранное для проверки время важном совещании с приглашением лиц из сторонних организаций. Ещё лучше, если руководство предприятия и в самом деле проведёт фиктивное, но правдоподобное совещание, способное настолько заинтересовать подслушивающего противника, что он активизирует все, включая дистанционно управляемые, средства НСИ. Очевидно, что выбранный сценарий мер по активации внедренных средств НСИ не должен противоречить легенде прикрытия поисковых мероприятий.

Важность всех этих вопросов для успеха проверки, их тесная взаимосвязь, влияние на обычный порядок работы предприятия и необходимость проработки в едином пакете требуют решений, принимать которые необходимо самому руководителю предприятия. Обычно руководитель предприятия будет стремиться переложить решение вопросов замысла на руководителя службы безопасности. Вместе с тем, именно руководитель предприятия наиболее полно представляет себе, откуда может исходить угроза его секретам, какая легенда прикрытия работ по проверке помещений наиболее органично впишется в деятельность предприятия, какой, не противоречащий легенде сценарий мер по активации средств НСИ следует предпочесть. Необходимо подчеркнуть, что сказанное выше относится, главным образом, к руководителю не очень крупной организации, имеющему возможность самому вникать во все нюансы её работы. На большом предприятии, где каждый крупный отдел, служба обычно разрабатывают собственные планы защиты информации, замысел проведения специальной проверки помещений отдела или службы может быть разработан руководителем этого подразделения.

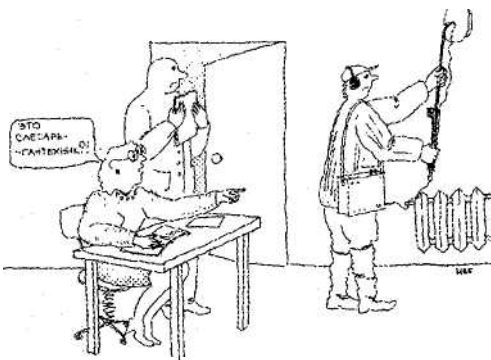
В любом случае специалисты службы безопасности должны помочь руководителю принять целесообразные решения по вопросам замысла специальной проверки помещений. В ходе обсуждения вопросов, относящихся к замыслу, специалисты должны помочь руководителю предприятия уяснить тесную взаимосвязь выбора времени проведения проверки, легенды прикрытия соответствующих работ и мер по активации внедрённых средств НСИ. Следует убедить руководителя в целесообразности выбора такой легенды прикрытия, которая позволяла бы использовать при проверке помещений, по возможности, весь арсенал поисковых средств.

Поясним это конкретным примером. Предположим, что легендой прикрытия поисковых работ помещений выбрана проверка функционирования пожарной и охранной сигнализации предприятия. Эта легенда допускает использование поисковой бригадой достаточно широкого спектра специальной техники. Вместе с тем, появление сотрудника с прибором нелинейной локации, обследующего стены и потолки помещений, не вписывается в содержание легенды. Такая легенда, если она выбрана как единственная, скорее всего, заставит отказаться от использования прибора нелинейной локации, а его отсутствие хотя бы частично компенсировать более тщательным визуальным осмотром и настойчивой рекомендацией руководителю предприятия установить в помещении систему активной защиты информации.

Целиком в компетенции руководителя предприятия находится также определение вариантов дальнейших действий в случае обнаружения средств НСИ. Обычно выбирается один из следующих вариантов:

- изъятие средства НСИ с места его обнаружения;
- нейтрализация средства НСИ без его удаления с места установки;
- сохранение средства НСИ в рабочем состоянии на месте обнаружения для последующего его использования в целях дезинформации противника.

При выборе варианта действий необходимо помнить, что *изъятие* средства НСИ может побудить противника к внедрению другого средства, для обнаружения которого придётся вновь проводить поисковые мероприятия.



*Нейтрализация* средства НСИ заключается в такой модификации его работы, при которой большинство функций средства сохраняются, кроме самого главного: оно перестаёт передавать противнику нужную ему информацию. Например, нейтрализация радиомикрофона может быть осуществлена путём заклеивания липкой лентой или заделки кусочком пластины отверстия для встроеного микрофона. Это приведёт к тому, что радиомикрофон будет продолжать свою работу до полного израсходования ресурса источника питания, но излучение радиомикрофона уже не будет модулироваться акустическими сигналами помещения. Нейтрализация средства НСИ является более скрытым от противника вариантом действий и потому более предпочтительным, однако, не снижает угрозу повторного внедрения противником аналогичного средства.

*Сохранение* средства НСИ *в рабочем состоянии* на месте обнаружения является наиболее скрытым от противника вариантом действий. В этом случае, однако, для ведения конфиденциальных переговоров в дальнейшем придётся выбирать другие помещения. Если же вы решите сохранить обнаруженное средство для последующей дезинформации противника, это потребует от вас разработки и проведения в жизнь специального сценария дезинформирующих мероприятий.

Текстуально оформленный замысел проведения проверки в последующем целиком войдёт в план проведения специальной проверки помещений в качестве его составной части.

#### 1.4. Изучение и предварительный осмотр объектов проверки.

Изучение и предварительный осмотр объектов проверки являются необходимыми условиями правильного определения объёма предстоящих работ и выбора необходимого оборудования. *Изучение* объекта проверки включает в себя:

- знакомство с профилем предприятия, особенностями его функционирования, назначением и особенностями использования подлежащих проверке помещений;

- изучение имеющихся планов территории предприятия, окружающей застройки, размещения на территории предприятия зданий и сооружений, размещения в зданиях помещений, подлежащих проверке и смежных с ними;

- изучение имеющихся на предприятии планов и строительных чертежей подлежащих проверке и смежных с ними помещений, другой строительной и ремонтной документации на эти помещения;

- знакомство организацией охраны территории предприятия, зданий и проверяемых помещений, изучение порядка и системы контроля доступа



на территорию предприятия, в подлежащие проверке и смежные с ними помещения;

- изучение схем инженерно-технических коммуникаций, энергоснабжения, связи, охранной, пожарной сигнализации, других документов, относящихся к работам по прокладке, ремонту и демонтажу проводных и инженерно-технических коммуникаций в подлежащих проверке и смежных с ними помещениях, обработке защищаемой информации в проверяемых помещениях;

- знакомство со сложившейся на предприятии системой защиты информации, используемыми техническими средствами защиты информации методами, принятыми по предотвращению утечки информации из подлежащих проверке помещений.

Изучение объекта проверки осуществляется путём его посещения, бесед с руководителем предприятия, руководителем службы безопасности предприятия, другими компетентными лицами, а также изучения имеющейся на предприятии документации. В ряде случаев, особенно когда на предприятии отсутствует необходимая проектная и эксплуатационная документация, документация устарела или её качество не удовлетворяет задачам проверки может возникнуть необходимость привлечь к собеседованию технических специалистов по эксплуатации зданий и технических систем: энергосистемы, системы центрального отопления, систем связи, радиотрансляции, электроснабжения и т. п.

Следует помнить, что все консультации и собеседования с компетентными лицами должны проводиться в рамках выбранных заранее легенд прикрытия (например, о предстоящем ремонте помещений или установке в них нового оборудования), чтобы не вызвать у собеседников подозрений о подготовке к проведению специальной проверки помещений.

В результате собеседований и изучения документов у специалистов поисковой бригады должно сложиться ясное представление о характере окружающей застройки и прилегающей местности, конструктивных и других особенностях здания, проверяемых и смежных с ними помещений, размещённом в них оборудовании, прохождении в проверяемых и смежных с ними помещениях проводных и инженерно-технических коммуникаций, доступности помещений для посетителей и персонала предприятия, системах охраны, контроля доступа и защиты информации. Этих представлений должно быть достаточно для составления перечня поисковых и исследовательских работ, плана необходимой для этих работ аппаратуры и ориентировочной оценки ожидаемых затрат на их выполнение.

Для сокращения и ускорения последующих работ целесообразно уже на этом этапе составить схему прилегающей к объектам проверки местности с указанием назначения, принадлежности и особенностей соседних строений,

поэтажные планы здания, в котором находятся подлежащие проверке помещения, и планы каждого проверяемого помещения. По каждому проверяемому помещению должна быть составлена его характеристика, включающая сведения о его назначении, размерах, особенностях ограждающих конструкций, мебелировке, других предметах обстановки, видах установленного оборудования, проводных и инженерно-технических коммуникациях и другие необходимые сведения. Аналогичные данные целесообразно подготовить и по смежным с проверяемыми помещениям.

Опыт проведения комплексных специальных проверок помещений показывает, что документальное изучение объектов проверки должно обязательно дополняться проведением их осмотра специалистами поисковых работ. Исключать предварительный осмотр объектов проверки из работ предварительного этапа нецелесообразно даже в тех случаях, когда на предприятии имеется полный комплект планов помещений и схем, позволяющий составить объективную картину предстоящей проверки. С какой бы тщательностью ни были составлены и изучены имеющиеся у предприятия планы помещений, схемы коммуникаций и другие документы, они не могут заменить информацию, получаемую специалистом по поиску при визуальном осмотре помещений.

Мы рекомендуем в ходе предварительного осмотра обратить особое внимание на следующее:

- влияние местности и окружающей застройки на прохождение радиоволн ультракоротковолнового диапазона и оптического излучения инфракрасного диапазона для определения возможных мест размещения противником пунктов приёма радиосигналов или инфракрасных излучений средств НСИ, а также пунктов перехвата ПЭМИ средств оргтехники из проверяемых помещений;
- возможность доступа посторонних лиц в зону электромагнитной доступности ПЭМИ средств оргтехники и излучений средств НСИ;
- возможность размещения средств съёма виброакустических сигналов на наружных поверхностях конструкций, ограждающих помещения, подлежащие проверке;
- конструктивные особенности проверяемых помещений и инженерно-технических коммуникаций, не отражённые в предварительно изученных документах (подшивные или подвесные потолки, подшивные стены, фальшполы, наличие подпольных каналов, плинтусов, съёмных панелей, наружных и скрытых кабельных каналов, трубопроводов, защитных экранов и т. п.);
- места возможного доступа посторонних лиц к элементам ограждающих конструкций помещений, технологическим и проводным коммуникациям, проходящим через подлежащие проверке помещения;
  - следы недавно проведённого ремонта, реконструкции или вторжения

в элементы ограждающих конструкций, инженерно-технических и проводных коммуникаций;

- особенности прокладки проводных коммуникаций, наличие линий, тратитом проходящих через проверяемые помещения;

- особенности внутреннего убранства и обстановки помещений (характер отделки стен, наличие напольных покрытий, количество мебели и её простота, количество и сложность предметов интерьера ит. д.).

В ходе осмотра следует иметь в виду, что в условиях неплотной городской застройке дальность приёма сигналов радиозакладки мощностью 20 Мвт, работающей в наиболее предпочтительном с точки зрения максимальной дальности распространения сигналов диапазоне 200.. 500 МГц, обычно не превышает 300.. 400м [12]. В условиях сплошной застройки при повышении рабочей частоты радиозакладки дальность приёма её сигналов существенно снижается. Напротив, в условиях прямой видимости между радиозакладкой и антенной радиоприёмного пункта дальность приёма её сигналов возрастает в два-три раза. Дальность перехвата ПЭМИ дисплеев ПЭВМ в условиях прямой видимости применения остронаправленных, антенн может достигать 400 м для дисплеев с металлическим кожухом и 1200 м для дисплеев с пластмассовым кожухом [20], однако обычно она редко превышает 50.. 80 метров.

Большим подспорьем в ходе дальнейших работ могут стать фотографии, которые можно сделать во время предварительного осмотра. Мы рекомендуем сделать фотографии окон наружных стен помещений, подлежащих проверке, в каждом помещении сделать несколько снимков его общего вида с различных точек съёмки, а также фотографии, фиксирующие расстановку мебели и других предметов интерьера в помещении, предметов на столах, полках и в шкафах. Не помешают и снимки заинтересовавших вас элементов строительных конструкций и коммуникаций. Результаты предварительного осмотра и изучения сделанных фотографий могут заметно повлиять на выбор поисковой и исследовательской аппаратуры, номенклатуру, содержание и тактику поисковых работ.

## 1.5. Выбор аппаратуры для проведения проверки, распределение сил и средств.

Важным элементом подготовки к проверке помещений является выбор технических средств, обеспечивающих проведение планируемых поисковых и исследовательских работ. В перечень аппаратуры, необходимой для проверки помещений на наличие средств НСИ, минимально должны входить:

- средства, обеспечивающие эффективность визуального осмотра элементов конструкции помещения, предметов интерьера и труднодоступных

ния мест;

- приборы для проверки проводных коммуникаций;
- аппаратура для выявления радиоизлучающих средств НСИ.

При проведении комплексных специальных проверок помещений этот перечень обычно дополняется металлоискателем, прибором нелинейной радиолокации и переносным рентгеновским комплексом.

В случаях, когда предварительный осмотр выявил необходимость проведения специальных исследований для выявления и оценки потенциальных ТКУИ, по согласованию с руководством предприятия в перечень необходимого оборудования включается аппаратура для проведения акустических и виброакустических измерений, исследования побочных электромагнитных излучений и другие необходимые приборы.

Мы рекомендуем совмещать проведение специальных проверок с контролем радиационной обстановки в помещениях. С этой целью в поисковой бригаде целесообразно иметь дозиметр или индикатор радиоактивного излучения. Примерный перечень специального оборудования и технических средств, рекомендуемых нами для проведения комплексной специальной проверки помещений, приведён в приложении 3.

Для каждого из выбранных типов приборов заранее должны быть продуманы необходимость и целесообразность дополнительных мер по активации внедрённых средств НСИ. В некоторых случаях, наоборот, может потребоваться введение ограничений на функционирование или даже размещение каких-либо средств на время работы с выбранным типом поисковой или исследовательской аппаратуры.

Поясним сказанное следующими примерами. Поиск информативных сигналов в линиях силовой и осветительной сети требует предварительного включения (активации) всех имеющихся в проверяемом помещении потребителей электроэнергии, а поиск информативных ПЭМИ ПЭВМ, наоборот, выключения всех остальных приборов и потребителей. Применение прибора нелинейной радиолокации для проверки элементов строительных конструкций требует предварительного удаления из зоны действия боковых лепестков его антенны оборудования и предметов, содержащих радиоэлектронные компоненты, в том числе, другой поисковой и исследовательской аппаратуры. В ряде случаев, например, при проверке



небольших по объёму серверных или других помещений со стационарно установленным радиоэлектронным оборудованием, эффективное применение этого прибора может вообще оказаться невозможным.

Комплексная специальная проверка помещений обычно проводится в условиях острого дефицита времени, отводимого на непосредственно поисковые исследовательские работы. Легенда прикрытия поисковых работ и меры по активации внедрённых средств НСИ не могут быть эффективными сколь угодно долгое время. В этой связи одной из проблем подготовительного этапа является правильное распределение имеющихся сил и средств по объектам проверки и видам работ. Под силами в данном случае следует понимать количество специалистов, включаемых в состав поисковой бригады. Очевидно, что чем значительнее будет состав бригады, тем меньше времени может занять непосредственное проведение проверки. Вместе с тем, неумеренное расширение состава поисковой бригады нецелесообразно из конспиративных соображений. Поэтому численный состав поисковой бригады должен определяться с учётом всех влияющих факторов.

Вынужденная из-за дефицита времени необходимость параллельного ведения различных работ в одних и тех же помещениях приводит к тому, что часть исследований придётся выполнять в условиях ограничений, накладываемых другими, проводимыми в то же время работами. Следует заранее продумать влияние этих ограничений на порядок работы с аппаратурой и приборами. В ряде случаев придётся внести коррективы в частные методики применения приборов. Выбранная легенда прикрытия и необходимость скрытного проведения работ также могут заставить изменить обычный порядок работы с некоторыми видами поисковой техники.

Известно, например, что поиск радиоизлучающих или использующих проводные коммуникации подслушивающих устройств заметно упрощается и ускоряется при использовании системы акустической обратной связи, имеющейся во многих поисковых приборах. В то же время, характерный звук работы этой системы позволяет подслушивающему противнику легко установить факт обнаружения внедрённого им устройства. По этой причине мы рекомендуем заранее отказаться от применения системы акустической обратной связи, невзирая на то, что это вызовет некоторое увеличение продолжительности поисковых работ.

Правильное распределение сил и средств невозможно без предварительной оценки затрат времени, требуемых для выполнения каждой из запланированных работ. Ожидаемые затраты времени могут быть определены методом экспертных оценок специалистами поисковой бригады с учетом накопленного опыта работ в ходе аналогичных проверок, объёма и других характеристик помещений, намеченных для проведения проверки.

Распределение имеющихся сил и средств по объектам проверки и видам работ должно проводиться в целях максимального сокращения общего времени

их проведения. Для оптимизации такого распределения мы рекомендуем воспользоваться известной методикой сетевого планирования работ. Тщательно продуманный сетевой график позволит согласовать в рамках единой структуры процесс проведения всех требуемых поисковых и исследовательских работ с учётом их объёма и взаимовлияющих ограничений. С учётом изложенных соображений мы рекомендуем следующий порядок действий:

- Определяются ориентировочные затраты времени для выполнения каждой из запланированных работ, в том числе, ожидаемая продолжительность работ с каждым из видов поисковой и исследовательской аппаратуры.
- Среди этих работ выделяются такие, одновременное проведение которых невозможно из-за их взаимоисключающего влияния или других соображений.
- Путём сложения определяются затраты времени, необходимые для последовательного выполнения работ, одновременное проведение которых невозможно.
- Отмечаются затраты времени на наиболее трудоёмкую из числа оставшихся работ.
- Определяется минимально возможная продолжительность непосредственного проведения специальной проверки, как наибольшая величина из затрат времени, определённых в двух предыдущих пунктах.
- В пределах минимально возможной продолжительности непосредственного проведения специальной проверки распределяются все запланированные работы таким образом, чтобы минимизировать количество одновременно (параллельно) выполняемых работ.

Полученное в результате этих манипуляций наибольшее число параллельно выполняемых работ укажет на минимально необходимый количественный состав поисковой бригады, который обеспечит проведение специальной проверки помещений за минимально возможное время.

## 1.6. Составление плана проведения специальной проверки.

План проведения комплексной специальной проверки помещений является генеральным документом, определяющим масштаб, конкретное содержание и методику проведения проверки. В случае, когда все изложенные в предыдущих разделах работы подготовительного этапа выполнены с требуемой тщательностью, составление и оформление этого плана не вызывает каких-либо трудностей. На наш взгляд, структура типового плана

проведения комплексной специальной проверки помещений должна  
выглядеть следующим образом (см. схему 2).

Схема 2

**Структура плана проведения  
комплексной специальной проверки  
помещений ||**

Выводы из оценки противника.

Замысел проведения специальной проверки помещений:

цель (побудительный мотив) проведения проверю!;

перечень и краткая характеристика проверяемых помещений;

перечень запланированных поисковых работ и исследований;

время проведения проверки;

легенда.

под прикрытием которой будет проводиться проверка;

меры по активизации внедренных средств НСИ;

действия в случае обнаружения средств НСИ.

Привлекаемые силы и средства, их распределение по объектам и видам работ

состав поисковой бригады;

привлекаемые для проведения проверки технические  
средствам основные особенности их применения,  
определяемые условиями проверки;

---

распределение сил и средств по объектам и видам работ;

---

дополнительные меры по активизации внедренных средств НСИ;

---

Перечень подготавливаемых по результатам проверки итоговых и отчетных документов и срок их представления для утверждения.

---

План мы рекомендуем оформлять в виде текстуального документа, включающего необходимые таблицы и поясняющие схемы.

В разделе выводов из оценки противника, оформляемом текстуально, целесообразно указать:

- категорию лиц, к которым может принадлежать субъект, выбранный вероятным противником для внедрения средств НСИ и съёма информации;
  - возможный уровень знаний, навыков и квалификации субъекта, осуществляющего внедрение средств НСИ;
- возможные виды применяемых средств НСИ, ожидаемая степень соответствия их характеристик наиболее продвинутым образцам аналогичных средств;
- возможные способы, время установки (внедрения) средств НСИ и действий по съёму информации;
  - вероятные действия в случаях установления намерений провести специальную проверку помещений, факта проведения такой проверки факта обнаружения внедрённых средств НСИ.

Все данные, необходимые для включения в этот раздел плана, уже были получены на этапе работ по выявлению вероятного противника и составлению модели его действий.

В раздел «Замысел проведения специальной проверки помещений» мы рекомендуем включить:

- цель (побудительный мотив) проведения специальной проверки помещений;
- оформленный в виде таблицы или текстуально перечень проверяемых помещений с краткой характеристикой каждого помещения: назначение, площадь и объём, особенности конструкции, основные виды обстановки, установленного оборудования и процент занимаемой ими общей площади (объёма) помещения, виды проводных технологических коммуникаций;
- перечень запланированных для каждого помещения поисковых работ и сопутствующих исследований (включая работы, намеченные к проведению в смежных помещениях и на наружных поверхностях ограждающих



строительных конструкций) с указанием их ожидаемой трудоёмкости;

■ время проведения специальной проверки помещений: дата, начало, конец; общая продолжительность непосредственного проведения проверки;

■ содержание и время действия легенды или нескольких легенд, под прикрытием которых будут проводиться работы по специальной проверке помещений, способы и начало доведения легенд до персонала предприятия, перечень оборудования и документов, необходимых для подтверждения легенд;

• меры по активации внедренных средств НСИ, способы и начало их выполнения;

• действия поисковой бригады в случае обнаружения средств НСИ.

Большинство данных, необходимых для разработки этого раздела плана, также было получено на предыдущих этапах подготовительных работ.

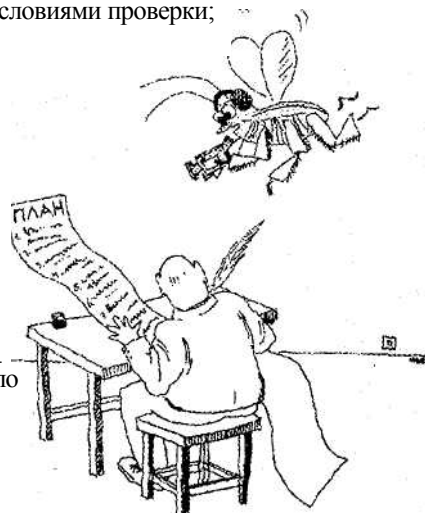
Раздел «Привлекаемые силы и средства, их распределение по объектам и видам работ», по нашему мнению, должен содержать:

• количественный и персональный состав поисковой бригады;

• перечень специального оборудования и технических средств, привлекаемых для проведения специальной проверки помещений с указанием основных особенностей их применения в различных вариантах выполнения легенд при различных условиях и других ограничений, налагаемых условиями проверки;

■ сетевой график выполнения запланированных поисковых и исследовательских работ или таблицу распределения специалистов поисковой бригады, оборудования и технических средств по видам работ и объектам специальной проверки;

• текстовую часть с изложением дополнительных мер по активизации внедренных средств НСИ в процессе применения конкретных типов поисковой аппаратуры.



Заключительный раздел плана проведения комплексной специальной проверки помещений должен содержать перечень подготавливаемых по результатам проверки итоговых и отчётных документов и срок их представления для утверждения. В этот перечень могут входить акт проведения

комплексной специальной проверки помещений, описание проведённых работ и исследований, протоколы измерений, рекомендации по повышению надёжности защиты информации от её возможной утечки по техническим каналам и другие документы.

Разработанный план утверждается руководителем предприятия. В ряде случаев, особенно в условиях острого дефицита времени при необходимости срочного проведения внеплановой специальной проверки, по договорённости с руководителем предприятия может оформляться сокращённый вариант плана. Иногда по той же причине и по соображениям конспирации допускается и устная форма представления плана.

Один из возможных вариантов плана проведения комплексной специальной проверки помещений приведёнными в приложении 5.

## 1.7. Предварительный анализ радиоэлектронной обстановки.

Предварительный сбор данных и анализ радиоэлектронной обстановки в районе проверяемых помещений - не обязательная, но весьма желательная фаза подготовительных работ. Она позволяет заметно ускорить последующие работы по радиомониторингу проверяемых помещений и повысить надёжность выявления радиоизлучающих средств НСИ.

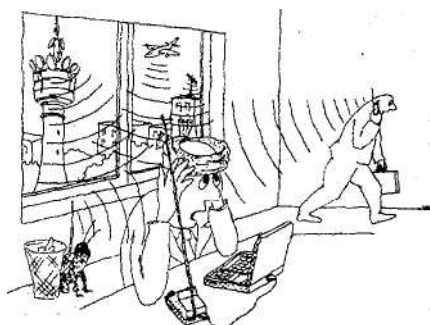
Предварительный сбор данных и анализ радиоэлектронной обстановки заключается в поиске, обнаружении радиоизлучений в районе проверяемых помещений, определении источников (принадлежности) обнаруженных радиоизлучений и их предварительной сортировке для последующего специального тестирования и анализа на принадлежность к излучениям средств НСИ и ПЭМИ средств оргтехники из проверяемых помещений. По согласованию с руководством предприятия дополнительными задачами анализа радиоэлектронной обстановки на этом этапе могут быть контроль соблюдения сотрудниками предприятия установленных его руководством ограничений на использование открытых каналов радиосвязи, контроль и оценка эффективности используемых технических средств защиты информации и другие задачи.

Проведение этих работ в условиях обычного режима деятельности предприятия позволяет составить карту занятости радиозфира, базу данных выявленных сигналов и исключить из последующего анализа известные радиоизлучения, существенно сократив время, требуемое для проведения радиомониторинга в процессе непосредственной проверки помещений.

Методика предварительного сбора данных радиоэлектронной обстановки и их анализа во многом определяется типами используемой аппаратуры.

Предварительный анализ радиоэлектронной обстановки

Минимально необходимый комплект оборудования должен включать широкодиапазонную антенну, сканирующий или перестраиваемый вручную радиоприёмник, имеющий непрерывный диапазон, как минимум, охватывающий области СВЧ (VHF), УВЧ (UHF) и начала СВЧ (SHF), канализатор спектра принимаемых сигналов. Работа с таким комплектом аппаратуры весьма трудоёмка, требует высокой квалификации и значительного опыта оператора.



В большинстве серьёзных организаций для ведения радиоконтроля и выявления радиолокационных средств используются автоматизированные программно-аппаратные комплексы, выполненные на базе ПЭВМ и сканирующего радиоприёмника. Такой комплекс обычно позволяет в автоматическом режиме снять панораму загрузки радиодиапазона, с минимальным участием оператора идентифицировать принимаемые излучения с сигналами известных источников (например, радиовещательных станций, систем телефонной сотовой или пейджинговой связи), провести ручной анализ остальных сигналов по их спектральным и другим характеристикам, составить списки частот идентифицированных излучений частот «подозрительных» сигналов.

Если служба безопасности предприятия не располагает собственным постом радиомониторинга, с руководителем предприятия должно быть согласовано место и время развёртывания временного пункта радиоконтроля, с комплектом необходимой радиоприёмной 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 развёрнутым в нём комплексом обнаружения радиоизлучающих средств и радиомониторинга КРОНА-6000М. Для выявления вблизи предприятия временного пункта радиоконтроля следует предусмотреть специальную легенду прикрытия, например, анализ органами радиоконтроля помеховой обстановки по заявке какой-нибудь сторонней организации.

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.

Можно рекомендовать следующий порядок работы на этом этапе:

- по согласованию с руководством предприятия определяется время начала, режим (круглосуточный или периодический) и продолжительность работы временного пункта радиоконтроля, место его развёртывания, перечень решаемых задач, легенда прикрытия работы;
  - в соответствии с объёмом и номенклатурой решаемых задач выбирается состав комплекта аппаратуры операторов пункта радиоконтроля;
  - с использованием имеющихся справочных данных (см. приложение 4), данных местного радиоклуба, рекламных публикаций и других источников осуществляется сбор и систематизация сведений о распределении занятости частот в регионе и, конкретно, в районе размещения проверяемых помещений;
  - составляется диаграмма (карта) занятости радиоэфир в виде частотной оси, на которой отмечаются границы и ведомственная принадлежность отдельных участков (диапазонов); такая нарезка общей полосы частот на отдельные участки позволяет осуществлять последовательный анализ их загрузки и облегчает определение принадлежности излучений в пределах каждого участка;
  - подготавливается таблица занятости частот с числом строк, равным ожидаемому количеству частот радиосигналов, и столбцами, в которых будут указаны частота излучения, принадлежность и отличительные особенности сигналов (вид модуляции, занимаемая полоса частот, относительный уровень, регулярность появления, время начала и длительность передачи и т. п.);
  - заполняется таблица занятости частот сведениями о сигналах известных источников радиоизлучения;
    - проводится необходимая подготовка аппаратуры, бланков документов для развёртывания и работы временного пункта радиоконтроля;
    - в запланированное время временный пункт радиоконтроля развёртывается и приступает к работе:
      - с использованием приёмо-анализирующей аппаратуры осуществляется последовательный просмотр реальной занятости отдельных участков диапазона с выявлением и анализом особенностей принимаемых сигналов для определения их принадлежности и идентификации с известными источниками излучений; сведения о параметрах и особенностях каждого излучения заносятся в таблицу занятости частот;
      - частоты сигналов, принадлежность которых выяснить не удалось, или которые идентифицируются с сигналами средств НСИ, заносятся в отдельный список для последующего наблюдения за ними и дополнительного анализа;
      - периодически (один - два раза в час) проводится повторный просмотр загрузки диапазонов для выявления и анализа новых излучений.
      - в промежутках между повторными просмотрами загрузки диапазонов осуществляется постоянный или периодический контроль занесённых в этот

этот список «подозрительных» частот с записью на регистрирующей аппаратуре проходящей информации с фиксацией времени начала и окончания работы источников излучений;

- по истечении времени, отведённого для предварительного сбора данных и анализа радиоэлектронной обстановки, временный пункт радиоконтроля свёртывается;

- в удобном месте, но не на глазах сотрудников предприятия операторы по результатам работы приёмо-анализирующей и документирующей аппаратуры проводят дополнительный анализ накопленных данных, оформляют таблицу занятости частот, уточняют список «подозрительных» частот, объём и методику предстоящей работы в ходе непосредственного проведения специальной проверки помещений.

Для выявления возможной связи появляющихся в эфире излучений с началом и режимом работы предприятия целесообразно приступать к контролю радио диапазона за один - два часа до начала рабочего дня на предприятии. Из этих же соображений завершать работу пункта радиоконтроля целесообразно не ранее, как через один - два часа после окончания рабочего дня и убытия с предприятия его руководства.

Следует иметь в виду, что для выявления радиоизлучений средств НСИ, осуществляющих накопление перехватываемой информации её передачу по расписанию, команде или радиозапросу ведущего разведку противника, необходимо круглоосуточнош радиомониторинг радиоэлектронной обстановки в районе проверяемых помещений. Организация круглосуточного функционирования пункта радиоконтроля требует особых мер конспирации, более тщательной подготовки аппаратуры и большего количества операторов, вследствие необходимости организовать их посменную работу. Вместе с тем, указанные средства НСИ встречаются достаточно редко из-за их высокой стоимости, сложности и немалых габаритов. Поэтому в некоторых случаях, допускаемых вашей оценкой финансово-технических возможностей противника, можно отказаться от ведения радиоконтроля в ночное время.

Таблицу занятости частот наиболее удобно составлять и вести в электронном виде с использованием ПЭВМ. Такая форма таблицы позволяет легко уточнять и упорядочивать данные, вставлять в соответствующие места таблицы необходимое количество дополнительных строк при появлении новых сигналов и источников радиоизлучений. При рукописной форме таблицы рекомендуется вести её на отдельных листах в скоросшивателе, обеспечивающем быструю замену или добавление новых листов.

При заполнении таблицы занятости частот сведениями об известных источниках радиоизлучений можно ориентироваться на приведённые в таблице 1 данные о зависимости дальности приёма стационарным пунктом радиоконтроля сигналов связанных радиостанций различной мощности от типа застройки окружающей местности [10].

Таблица 1

Ожидаемые дальности приёма сигналов станций радиосвязи  
В процессе анализа сигналов следует иметь в виду, что часть из них

Тип застройки	Стационарные радиостанции	Автомобильные радиостанции	Портативные радиостанции
Малоэтажная (1-3 эт.)	70 км	15...20 км	10...15 км
Среднеэтажная (до 9 эт.)	50 км	10...15 км	5...10 км
Многоэтажная (выше 9 эт.)	30 км	5...10 км	3...5 км

может оказаться побочными или внеполосными излучениями расположенных невдалеке мощных радиопередатчиков, излучениями промышленного или других видов оборудования. Идентификация таких сигналов с известными источниками представляет определённые трудности, но может быть осуществлена путём сопоставления их частот, времени появления и других особенностей. Сигналы на выходе радиоприёмника могут быть также следствием несовершенства самой радиоприёмной аппаратуры, например, из-за наличия побочных каналов приёма или перекрёстной модуляции сигналов во входных цепях. Поэтому оператор должен иметь полное представление о недостатках используемой аппаратуры.

Определение принадлежности излучений облегчается, если используемая техника имеет высокую разрешающую способность и позволяет анализировать, документировать и сопоставлять максимальное количество параметров принимаемых сигналов. Большим подспорьем для оператора может стать «библиотека» спектров, осциллограмм и фонограмм характерных источников радиоизлучений: радиорелейных линий связи, организационных каналов сетей сотовой связи и т. п. Сопоставлением обнаруженных излучений с образцами сигналов известных источников можно с высокой степенью достоверности идентифицировать значительное количество неизвестных сигналов.

Известно, что радиоизлучающие средства НСИ в спектре своего излучения обычно имеют большое количество гармоник основной (несущей) частоты. Поэтому рекомендуется проверять «подозрительные» сигналы на наличие гармоник выявленной частоты и проводить оценку их относительных уровней. В случаях, когда источники излучений имеют высокий уровень гармоник основной частоты, а время их работы и прохождения по ним информации совпадает со временем работы предприятия, можно сделать вывод о возможной принадлежности обнаруженных излучений к сигналам периодически включаемых средств НСИ или побочным излучениям средств оргтехники, работающих на этом предприятии. Естественно, что сигналы на этих частотах должны быть проанализированы и протестированы особенно тщательно при

радиомониторинге помещений во время непосредственного проведения их специальной проверки.

## 1.8. Завершающие работы подготовительного этапа.

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.

В качестве документов, подтверждающих выбранные легенды прикрытия, могут использоваться:

- наряд, заказ-наряд или копия договора на проведение работ;
- допуск для работы на оборудовании и в определённых помещениях;
- счет-фактура на выполняемые работы;
- технологические карты для выполнения отдельных видов работ;
- накладные на устанавливаемое оборудование и аппаратуру;
- формуляры, бланки протоколов измерений и отчетных документов, техническая и методическая литература, подтверждающая выбранную легенду прикрытия.

Документы должны быть изготовлены в требуемом количестве экземпляров надлежащим образом оформлены, в том числе, необходимыми подписями должностных лиц предприятия.

Для сокращения непроизводительных затрат времени в ходе непосредственного проведения специальной проверки помещений целесообразно заранее подготовить:

- схемы коммуникаций и планы проверяемых помещений, на которые будут наноситься отметки мест обнаружения средств НСИ и подозрительных мест;
- бланки протоколов будущих измерений;
- журнал регистрации заводских инвентарных номеров проверенного оборудования;
- журналы регистрации мест установки пломб и скрытых меток, способствующих ускорению работ при проведении их специальной проверки;
- карту занятости радиоэфира;
- базу данных выявленных и идентифицированных радиосигналов;
- список частот «подозрительных» радиоизлучений.

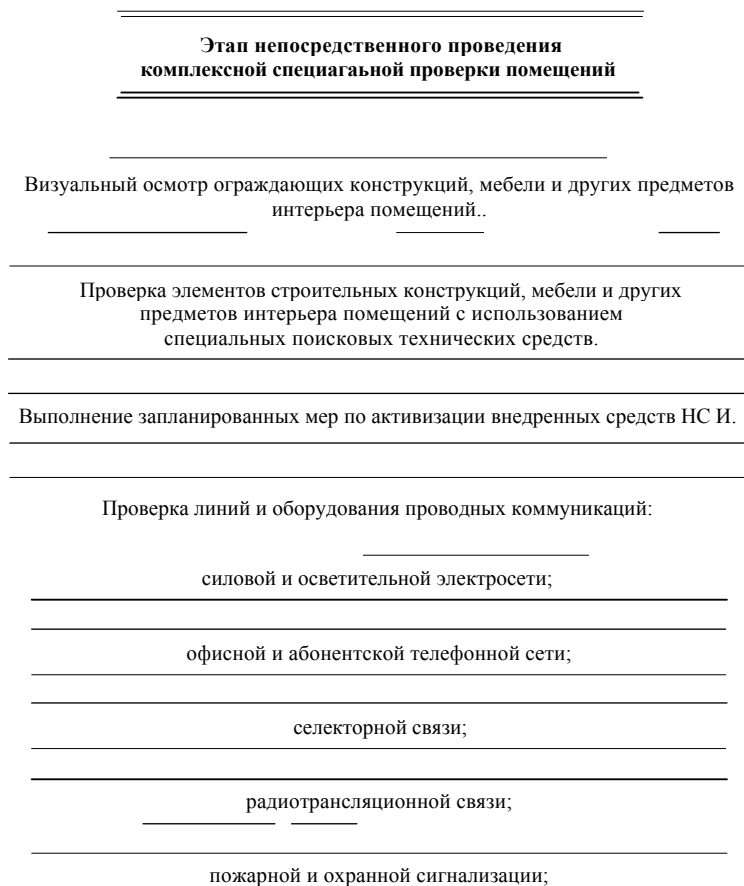
Следует помнить, что в отличие от документов, подтверждающих легенды прикрытия, все документы, подготавливаемые для работ по непосредственному проведению проверки, относятся к категории строго

конфиденциальных и не подлежат разглашению среди сотрудников предприятия.

## 2. Этап непосредственного проведения комплексной специальной проверки помещений.

Непосредственное проведение в помещениях запланированных поисковых мероприятий и исследований составляет содержание второго этапа работ по комплексной специальной проверке помещений. Виды работ, которые могут проводиться на этом этапе, представлены на схеме 3.

Схема 3





системы часофикации;

---

других проводных коммуникации, в том числе,  
невьясненного назначения.

---

Радиомониторинг проверяемых помещения.

---

Поиск средств негласного съема и передачи информации, внедренных в  
электронные приборы.

---

Исследование звукопроницаемости элементов конструкций, проверка  
трубопроводных и других инженерно - технических коммуникаций на  
наличие в них акустических и виброакустических сигналов  
из проверяемого помещения.

---

Исследование побочных электромагнитных излучений компьютеров,  
оргтехники и другого оборудования для выявления в них  
информативных сигналов.

---

Г

Необходимо заметить, что последние два вида работ могут не входить в программу комплексной специальной проверки помещений так как не относятся к поиску внедрённых средств НСИ. Тем не менее, при необходимости данные исследования могут быть проведены с помощью специальной исследовательской аппаратуры по методикам, раскрытие которых мы оставляем за рамками данной публикации.

Перед началом непосредственного проведения поисковых работ рекомендуется осмотреть прилегающие к месту проведения работ территорию для обнаружения возможно развёрнутых противником постов приёма информации из подлежащих проверке помещений. Подозрения должны вызывать лица, пользующиеся наушниками, а также автомобили, длительно находящиеся с людьми на одном месте. Особое внимание следует обратить на автомобили с внешней антенной, вставленным в гнездо прикуривателя адаптером, тонированными или занавешенными окнами. Рекомендуется записать номера вызвавших подозрение автомобилей, приметы находящихся в них людей и других подозрительных лиц. В случае обнаружения в помещениях средств НСИ эти сведения могут пригодиться для установления конкретных лиц и организаций, причастных к негласному съёму защищаемой информации.

В проверяемом помещении рекомендуется закрыть двери, окна, жалюзи и шторы для исключения визуального контакта с возможными наблюдателями со стороны улицы или из соседних помещений. Для маскировки шумов, сопровождающих ведение поиска, целесообразно включить магнитола, радиоприёмник или другую звуковоспроизводящую аппаратуру. Развертывание поисковой и исследовательской аппаратуры и ведение запланированных работ должно осуществляться, по возможности, бесшумно, с выполнением демонстрационных действий, предусмотренных легендой прикрывающей работ.

## 2.1. Визуальный осмотр ограждающих конструкций, мебели и других предметов интерьера помещений.

Визуальный осмотр ограждающих конструкций, мебели и других предметов интерьера помещений наличие в них средств НСИ является обязательным необходимым элементом поисковых работ. Тщательный осмотр всегда связан с перемещением мебели и предметов, которые по окончании проверки помещения должны быть оставлены в том положении и виде, в каком они находились до начала осмотра. Поэтому перед началом осмотра проводится протоколирование и фотографирование размещения всех предметов, находящихся в помещении.

Основным методическим приёмом, используемым в ходе проведения осмотра знакомого, ранее уже проверявшегося помещения, является переход от общего к частному. На практике это означает, что вначале следует обратить внимание на особенности и изменения внешнего вида стен, пола, потолка помещения, расстановки в нём мебели и других крупных предметов интерьера, размещения напольных покрытий. При этом используются ранее заготовленные планы помещения, схемы расстановки мебели и предметов, фотографии, сделанные во время предыдущей проверки помещения или его предварительного осмотра. Затем переходят к выявлению особенностей и изменений в размещении предметов на столах, в шкафах, на стенах, подоконниках,



выявлению новых, недавно появившихся предметов. Завершают осмотр детальным исследованием внешних поверхностей, поло стей и внутренних поверхностей каждого предмета, элемента интерьера и конструкции помещения. В необходимых случаях используются фонари, досмотровые зеркала, лупы, эндоскопы.

При необходимости работы в малознакомом для членов поисковой бригады помещении мы рекомендуем предварительно условно разбить его объём наряд отдельных участков (фрагментов) и осуществлять осмотр этих участков по заранее составленной схеме, например, от окна или входной двери по часовой стрелке, снизу вверх, от периферии к центру помещения. Тем самым снижается вероятность случайного пропуска какого-либо участка или предмета во время осмотра. Если по результатам предварительного осмотра помещения не удалось составить его подробный план, схемы расстановки мебели и предметов, эти документы необходимо изготовить или уточнить сейчас, в ходе визуального осмотра помещения.

В процессе осмотра следует искать новые, ранее не присущие данному помещению, возможно подброшенные предметы, а также признаки возможного использования элементов интерьера и конструкции помещения для внедрения в них средств НСИ. К таким признакам относятся:

- перестановка мебели и предметов, появление на них новых, ранее не отмечавшихся элементов и деталей;
- смещение предметов, покрытий и мебели с их обычных мест;
- следы вскрытия панелей и других съёмных элементов конструкции помещения и предметов;
- следы недавней заделки отверстий, оштукатуривания или свежей окраски поверхностей и т. п.

В ходе осмотра целесообразно периодически представлять себя в роли вероятного противника, моделируя его возможные действия по внедрению средств съёма информации. Для повышения реалистичности модели необходимо учитывать время, которым мог располагать противник для установки подслушивающих или подглядывающих устройств, его профессиональные навыки и другие факторы.

В процессе осмотра целесообразно на заранее заготовленном плане помещения делать отметки подозрительных мест, нуждающихся в дополнительном, более тщательном обследовании с помощью специальных поисковых технических средств. Не следует, однако, слишком полагаться на возможности поисковых технических средств, поскольку некоторые средства НСИ практически не удаётся обнаружить ни одним типом поисковой аппаратуры. В качестве примера таких средств НСИ укажем на оптоволоконный микрофон, представляющий собой длинный тонкий световод с чувствительной к акустическим колебаниям мембраной на конце.

По световоду подаётся лазерное излучение. Отражаемое мембранной излучение оказывается промодулированным акустическими колебаниями. Такой микрофон практически не имеет демаскирующих его физических полей и может быть обнаружен только визуальным осмотром.

Для детального осмотра ограждающих помещения конструкций мебель и другие предметы интерьера следует отодвинуть от стен и окон. Необходимо обеспечить доступ для осмотра имеющихся в помещении ниш, подпольных каналов, плинтусов, вентиляционных коробов, технологических отверстий. Особое внимание следует уделить съёмным и пустотелым элементам конструкций: декоративным стеновым панелям, металлическими пластиковым трубчатым конструкциям, подвесным потолкам, элементам пластиковых оконных рам, плинтусам и наличникам, съёмным элементам декора, имитирующим лепнину.

В ходе осмотра элементов конструкции помещения следует также обращать внимание на их звукопроницаемость, электропроводность, способность передавать акустические и вибрационные сигналы за пределы помещения. Это необходимо для выявления и оценки на качественном уровне акустических воздушных, акустических вибрационных, электромагнитных потенциальных ТКУИ, определения возможности использования противником электропроводящих элементов конструкции помещения и элементов инженерно-технических коммуникаций для съёма наводок или передачи из помещения электрических сигналов средств НСИ.

Приведём ряд частных методических рекомендаций по проведению визуального осмотра некоторых типовых элементов конструкции помещения и инженерно-технических коммуникаций с целью выявления внедрённых средств НСИ.

При *визуальном осмотре пола* мы рекомендуем:

- приподнять и осмотреть снизу напольные покрытия (ковры, паласы, линолеум и т. п.), обращая внимание на нехарактерные для данного покрытия участки: вставки, подклейки, заплатки;
- осмотреть поверхность пола, исследовать места со следами недавней покраски, ремонта, применения инструмента, нарушающего целостность поверхности;
- в случае паркетного, плиточного или другого наборного настила проверить надёжность крепления его элементов, отсутствие следов применения нехарактерных для основной площади пола связующих материалов (клея, цемента, затирки и т. п.) и других следов возможного вскрытия и последующего заделывания поверхности;
- осмотреть плинтусы, тщательно исследовать места со следами недавнего ремонта и возможного вторжения, в необходимых случаях провести их временный демонтаж для осмотра пространства под плинтусами, убедиться в отсутствии под плинтусом скрытых электропроводящих и оптоволоконных

- вскрыть и осмотреть подпольные каналы, обращая особое внимание на нижнюю сторону съёмных крышек, имеющиеся пазы и щели, следы их недавней заделки; тщательно, на максимально возможную глубину с применением эндоскопа осмотреть содержимое труб, подходящих к подпольным каналам, убедиться в отсутствии в них посторонних предметов и проводов; штатные провода кабелей в ходе осмотра рекомендуется вытянуть из закладных труб (кабельных каналов) на максимально возможную длину для того, чтобы убедиться в отсутствии несанкционированных подключений к проводам;
- тщательно осмотреть места сквозного прохождения через пол водопроводных труб, труб парового отопления и других коммуникаций, поскольку в этих местах наиболее просто замаскировать следы вторжения при установке средств НСИ.

*Визуальный осмотр стен* для сокращения времени осмотра целесообразно совмещать с осмотром развешенных на них предметов интерьера и покрытий. Рекомендации по осмотру предметов интерьера приведены ниже, а пока рассмотрим методику визуального осмотра стен. При осмотре стен необходимо:

- освободить их поверхность от навешенных предметов и покрытий (картин, зеркал, ковров ит. п.);
  - осмотреть поверхность стен, обращая особое внимание на места, отличающиеся по своей окраске или фактуре от остальной поверхности; отметить подозрительные места на плане помещения для последующего их исследования с помощью специальных технических средств;
  - в случае оклейки поверхности стен обоями тщательно осмотреть места неровностей, стыков обоев, заплат, порезов и надрывов, убедиться в плотности прилегания обоев к поверхности стены; при необходимости вскрыть отслоившиеся обои для проверки содержимого образовавшейся полости;
  - при наличии съёмных, декоративных панелей, планок и бордюров внимательно осмотреть их поверхность в местах стыков для обнаружения следов возможного демонтажа и внедрения средств НСИ, проверить наличие и состояние специальных меток, оставленных в ходе последней специальной проверки помещения; в подозрительных случаях снять панели, осмотреть их внутренние поверхности, за панельные полости и поверхность стены за панелями; по окончании осмотра установить съёмные элементы на место, нанести новые метки для облегчения контроля за неприкосновенностью элементов в ходе последующих проверок, зафиксировать места нанесения метки их характеристику в специальном журнале;
  - в случае подшивных стен особое внимание обратить на наличие следов высверливания и последующего заделывания отверстий;
  - при наличии в стенах технологических, коммуникационных и других

нищ, закрываемые съёмными крышками или панелями, осмотр ниш и проводов в соответствии с рекомендациями по осмотру подпольных каналов.

При *визуальном осмотре* вентиляционных и других технологических *отверстий и полостей* мы рекомендуем:

- проверить неприкосновенность закрывающей отверстие решётки или крышки по нанесённым в ходе предыдущей проверки специальным меткам;
  - снять закрывающую отверстие решётку, убедиться в отсутствии следов нарушения пылевого слоя вокруг отверстия и на внутренних его поверхностях;
- убедиться в отсутствии посторонних предметов и проводов в отверстии, полостях и подходящих к полости трубах, для чего использовать досмотровые зеркала, эндоскопы и фонари.

При *визуальном осмотре окон* необходимо:

- провести осмотр поверхностей подоконника, оконного проёма и оконной рамы, обращая особое внимание на имеющиеся щели и полости, плотность прилегания и однородность крепления уплотнений, следы нарушения целостности поверхности;
  - открыть окно и убедиться в отсутствии посторонних проводников и предметов на внутренних и наружных поверхностях оконной рамы, следов демонтажа или замены уплотнений, запорных элементов, элементов крепления;
  - в случае двойных рам провести их разборку, убедиться в отсутствии посторонних проводников и предметов в межрамных щелях;
    - при использовании конструкции рам алюминиевых, пластиковых и других профильных элементов убедиться в отсутствии следов демонтажа или замены этих элементов, при необходимости провести разборку рам с исследованием внутренних полостей профильных элементов с помощью досмотровых зеркал и эндоскопа;
    - внимательно осмотреть все поверхности и полости карнизов, жалюзи, складки штор, убедиться в отсутствии посторонних предметов;
  - осмотром прилегающих к оконному проёму участков наружных стен убедиться в отсутствии на них посторонних предметов, заплат или других следов возможного вторжения; особое внимание следует обратить на участки, скрытые от поверхностного осмотра отбойными козырьками.

В большинстве помещений под окнами размещены радиаторы системы парового отопления. Сложная конфигурация радиаторов, часто встречающееся применение декоративных экранов, скрывающих радиаторы и трубы системы отопления от наблюдения, создают благоприятные условия для установки в этих местах средств НСИ. Осмотр таких мест должен проводиться с особой тщательностью, с применением фонаря и

досмотровых зеркал, с обязательным демонтажем и осмотром декоративных экранов. Обнаружение на радиаторе или элементах трубопроводов вставок или нештатных, недавно появившихся деталей должно стать причиной детального их исследования с применением, в случае необходимости, специальных поисковых технических средств. При *визуальном осмотре дверей* мы рекомендуем:

- осмотреть щели за наличниками дверной коробки, убедиться в отсутствии следов демонтажа наличников; в случае подозрений на их вскрытие демонтировать наличники, осмотреть скрытые ими пазы и щели, убедиться в отсутствии следов их недавней заделки;
  - убедиться в отсутствии следов вскрытия дверной обивки и дверного полотна, в подозрительных случаях снять и осмотреть обратную сторону дверной обивки и скрытую обивкой поверхность дверного полотна;
  - осмотреть элементы навески двери и убедиться в отсутствии следов их демонтажа; в случае подозрений демонтировать дверные петли и осмотреть скрытую за ними поверхность дверной коробки или дверного полотна;
- при осмотре металлической двери обратить особое внимание на следы высверливания отверстий в дверном полотне и дверной коробке, следы временного демонтажа запорных элементов и элементов навески двери; в подозрительных случаях демонтировать замок и осмотреть внутренние полости дверного полотна с помощью эндоскопа.

При *визуальном осмотре потолка* следует обратить внимание на участки со следами недавней покраски, ремонта, протечек, сквозного прохождения труб и других коммуникаций. Особого внимания требует осмотр подвесного потолка. Такой потолок состоит из съёмных, закрепляемых на каркасе панелей и легко может быть использован злоумышленником для установки средств НСИ. В большинстве случаев осмотр такого потолка весьма трудоёмок и требует хотя бы частичного его демонтажа. Необходимо также иметь в виду, что дополнительная проверка такого потолка с помощью прибора нелинейной радиолокации очень часто не даёт удовлетворительных результатов из-за ложных срабатываний, вызываемых большим количеством металлических, покрытых коррозией деталей и проволочных скруток. Осмотр подвесного потолка, как правило, совмещается с визуальным осмотром и проверкой линии установленного на потолке оборудования проводных коммуникаций.

Перед вскрытием потолочных панелей следует убедиться в целостности меток, оставленных в ходе предыдущей проверки. В случае нарушения меток или обнаружении следов возможного вскрытия панелей осмотр за панелью пространства следует начать с подозрительных мест. При вскрытии панелей прежде всего осматривается их обратная сторона. Особое внимание следует уделить осмотру пазов и неосматриваемых снизу поверхностей каркаса. Использование досмотровых зеркал при этом совершенно необходимо. Для

выявления несанкционированных подключений тщательно осматриваются скрытые панелями подвесного потолка провода и другие элементы систем освещения, пожарной и охранной сигнализации, связи. В процессе осмотра за панелью пространства проводится параллельный осмотр с демонтажем и разборкой осветительных, сигнализационных и других приборов, смонтированных на потолке.

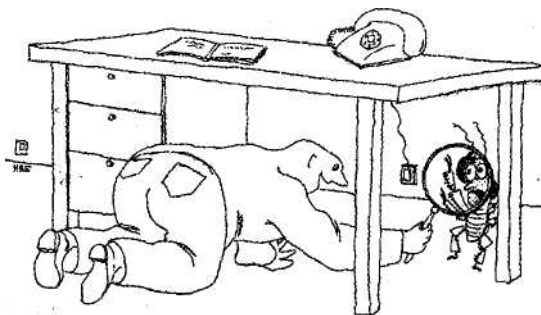
Высокие трудозатраты, связанные с визуальным осмотром подвесного потолка, требуют с особой тщательностью продумать технологию нанесения скрытых меток на устанавливаемые панели для облегчения последующего контроля их неприкосновенности. Виды меток, места и способы их нанесения обычно определяются на месте членом поисковой бригады и заносятся в виде схем, рисунков и пояснительного текста в специальный журнал регистрации пломб и скрытых меток.

Параллельно с осмотром ограждающих конструкций или по его завершении проводится *визуальный осмотр мебели* и других предметов интерьера. Осмотр мебели, как и помещения, обычно проводится от общего к частному: вначале осматриваются внешние поверхности основных конструктивных элементов, затем - съёмных и внутренних элементов, заканчивается осмотр исследованием пазов, отверстий и внутренних полостей. Практика поисковых работ показывает, что наиболее часто для установки средств НСИ используются кресло, стол и шкаф руководителя, стол для проведения совещаний, сейф, холодильник. Визуальный осмотр мебели проводится в следующей последовательности:

- поверхности мебели (полки, ящики, сиденья и т. п.) освобождаются от предметов и покрытий, выемные и легко съёмные элементы удаляются для отдельного осмотра;
- осматриваются поверхности основных конструктивных элементов для выявления закреплённых посторонних предметов и деталей, отверстий неясного назначения, вставок, наклеек, швов, других следов вторжения; особое внимание уделяется сравнению толщины стенок и панелей, осмотру задних и нижних поверхностей элементов, пазов и щелей, а также складки швов обивки мягкой мебели;
- осматриваются поверхности крепёжных и соединительных элементов для обнаружения следов возможного демонтажа мебели с целью скрытия за соединительными элементами средств НСИ; для облегчения последующего контроля неприкосновенности крепёжных и соединительных элементов целесообразно покрыть головки крепёжных деталей и места соединения элементов тонким слоем маркирующей краски;
- проводится осмотр наружных и внутренних поверхностей выемных и легко съёмных элементов в соответствии с рекомендациями по осмотру основных конструктивных элементов;
- с помощью досмотровых зеркал и эндоскопов осматриваются



д оступные отверстия полости мебели; неразъёмные элементы конструкции мебели, вызывающие подозрение, и недоступные полости оставляются для дополнительного обследования с помощью специальных технических средств неразрушающего контроля.



Некоторые особенности имеет методика осмотра встроенной мебели. Обычно в виде встроенной конструкции выполняются платяной и книжный шкафы, стеллажи для документации, сейф. Основным отличием встроенной мебели является её стационарное размещение и невозможность отделения от стен помещения, поэтому осмотр встроенной мебели может проводиться одновременно с осмотром ограждающих помещение конструкций. В ходе осмотра встроенной мебели особое внимание уделяется исследованию декоративных покрытий и элементов конструкции, образующих заднюю стенку мебели, поскольку они могут скрывать полости, удобные для установки средств НСИ. При осмотре такой мебели целесообразно прощупать и простучать наклеенные внутри обои, демонтировать внутренние декоративные покрытия и исследовать скрытые за ними щели и полости.

После завершения осмотра мебели, а иногда параллельно с ним проводится визуальный осмотр других предметов интерьера помещения: отдельно стоящих на полу, развешенных на стенах, размещённых на подоконниках или поверхностях мебели. Ввиду огромного многообразия предметов невозможно подробно описать особенности осмотра каждого из них, поэтому остановимся лишь на наиболее общих моментах методики их осмотра.

Визуальному осмотру подлежат не только предметы интерьера помещения, но также предметы, являющиеся содержимым ящиков столов, шкафов и другой мебели, карманов хранящейся в помещении одежды и других ёмкостей. Методика визуального осмотра этой категории предметов не отличается принципиально от методики осмотра предметов интерьера помещений, поэтому изложенные выше рекомендации применимы для неё.

Осмотр предмета начинается с оценки возможности его использования, как объекта для внедрения противником средства НСИ. В случае положительной оценки проверяется подлинность предмета для исключения вероятности его подмены и выявляются следы возможного вскрытия предмета противником. Рассмотрим в качестве наиболее общего случая последовательность визуального осмотра предмета сложной конструкции,

имеющего съёмные, разборные и пустотелые элементы. Для осмотра такого предмета необходимо:

- проверкой инвентарного номера и специально нанесённых скрытых меток убедиться в подлинности предмета и отсутствии его подмены;
- внешним осмотром наружных поверхностей предмета убедиться в отсутствии новых дополнительных элементов, наклеек, следов сверления, взлома или других способов проникновения внутрь предмета; проверить целостность пломб и специальных меток, нанесённых на съёмные детали, крышки и панели предмета для облегчения контроля его неприкосновенности;
- в случае нарушения пломб или обнаружения других следов вскрытия предмета провести демонтаж съёмных деталей для осмотра этих деталей и внутренних полостей предмета; особое внимание следует обращать на наличие вставок, наклеек, следов монтажной пены, новых, нестандартных или отличающихся по фактуре, цвету и другим параметрам деталей, не присущих данному предмету;
- при необходимости провести полную разборку предмета с осмотром всех его элементов и исследованием пазов, щелей и полостей с помощью лупы, досмотровых зеркал, эндоскопа или других поисковых технических средств;
- по завершении осмотра провести сборку деталей предмета с нанесением скрытых меток и установкой специальных пломб, облегчающих последующий контроль неприкосновенности предмета.

С особой тщательностью следует осматривать предметы, постоянно находящиеся на столе или в непосредственной близости от рабочего стола руководителя. Широкое распространение стандартных канцелярских приспособлений и приборов облегчает их замену на аналогичный прибор, но суживает возможности средств НСИ. Поэтому все предметы интерьера должны иметь индивидуальные инвентарные номера и скрытые опознавательные метки, нанесённые, например, специальным маркером, следы которого проявляются только в ультрафиолетовых лучах. Осмотру и проверке подлежат папки с документацией, книги, рамы картин и зеркал, корзины для мусора, цветочные горшки комнатных растений, часы, статуэтки и другие предметы, имеющие внутри себя полости, размеры которых позволяют разместить в них средства НСИ.

Существенные особенности имеет поиск средств НСИ, внедрённых в электронные приборы, поэтому рекомендации по такому поиску будут рассмотрены в отдельном разделе.

Подчеркнём ещё раз, что визуальный осмотр следует проводить не только в тех помещениях, на которые указал руководитель предприятия, заказавший проверку, но и в смежных с ними. В них должны быть осмотрены общие с основным помещением (смежные) стены и другие элементы ограждающих

конструкций, смежные полости, вентиляционные короба, дымоходы, кабельные каналы и другие технологические каналы и отверстия, общие элементы трубопроводных коммуникаций (водопровода, парового отопления, канализации). Осмотрены должны быть также наружные (уличные) поверхности стен и других ограждающих помещения строительных конструкций.

Накопленный опыт проведения комплексных специальных проверок помещений позволяет утверждать, что тщательный визуальный осмотр может выявить практически все типы подбрасываемых средств НСИ и подавляющее большинство средств НСИ, требующих незначительного времени для их установки. Для некоторых видов средств НСИ визуальный осмотр является единственным способом их обнаружения. Вместе с тем он весьма трудоёмок и требует разборки, а иногда и разрушающего вмешательства в предмет или конструкцию для снятия возникших подозрений, поэтому визуальный осмотр целесообразно сочетать с применением специальной аппаратуры неразрушающего контроля подозрительных мест.

В заключение хотелось бы подчеркнуть, что обнаружение вами замаскированного диктофона, подброшенного радиомикрофона или другого средства НСИ не должно стать причиной поверхностного выполнения остальных предусмотренных планом поисковых работ, тем более, их свёртывания и прекращения. Следует помнить о таком общеизвестном тактическом приёме, как «отвлекающий маневр», более известный среди сотрудников спецслужб под названием «отвлечение на негодный объект». Весьма вероятно, что противник установил не одно, а два или даже несколько дублирующих друг друга средств НСИ как раз в расчёте на то, что после обнаружения одного, из них поисковая бригада ослабит или вообще свернёт дальнейший поиск. Уверенность в «чистоте» проверяемого помещения может дать только полное и тщательное выполнение всех запланированных поисковых работ.

## 2.2. Проверка элементов строительных конструкций, мебели и других предметов с использованием специальных технических средств.

В процессе визуального осмотра ограждающих конструкций, мебели и других предметов интерьера помещений, как правило, выявляется большое количество мест, вызывающих подозрение по тем или иным внешним признакам. Далеко не всегда возможно и целесообразно рассеять возникшие подозрения путём взлома стены, мебельной панели или вскрытия пола. Во всех этих случаях более рациональным считается применение специальных

технических средств неразрушающего контроля: обнаружителей пустот, металлодетекторов, приборов нелинейной радиолокации, флуороскопов, рентгенотелевизионных комплексов.

Обнаружители пустот позволяют обнаружить скрытые в толщине стен, за облицовочными панелями и другими преградами полости, возможно использованные для размещения средств НСИ. Металлодетекторы (металлоискатели) реагируют на наличие токопроводящих объектов в диэлектрической среде и помогают выявить корпуса и другие металлические элементы средств НСИ в неметаллических конструкциях и предметах. Приборы нелинейной радиолокации регистрируют наличие нелинейных преобразований в отражённом предметами зондирующем сигнале и дают возможность обнаружить и локализовать электронные средства НСИ по входящим в их состав полупроводниковым элементам. Флуороскопы и рентгенотелевизионные комплексы дают светотеневое изображение внутренней структуры объекта контроля при его облучении рентгеновским излучением и применяются в случаях, когда назначение найденного предмета не удаётся установить без его разрушения.

Подробные методики практического применения данных технических средств приведены в соответствующих руководствах и инструкциях по эксплуатации конкретных типов этой аппаратуры. В рамках данной брошюры остановимся лишь на наиболее общих моментах методики поиска средств НСИ с использованием этой техники.

Принцип действия обнаружителей пустот основан на использовании и выявлении различий в акустических свойствах, диэлектрической проницаемости или теплопроводности воздуха (пустоты) и сплошной среды. При использовании акустического, в том числе, ультразвукового обнаружителя пустот датчик-преобразователь прибора перемещают вдоль поверхности стены в разных направлениях и определяют по изменению громкости отраженного звука, пикам кривой эхосигналов на экране осциллоскопа или яркости отметок на экране прибора наличие и размеры (границы) полости. В высокочастотных электромагнитных обнаружителях пустот вдоль поверхности стены или конструкции перемещают зонд, в виде которого выполнен контур высокочастотного генератора прибора. Изменение частоты генератора может свидетельствовать о наличии в районе размещения зонда скрытой полости. Общим недостатком обнаружителей пустот является то, что они регистрируют не только наличие пустот, но и простых неоднородностей в конструкциях. По этой причине обнаружители пустот используются лишь в качестве дополнительных средств к другим видам поисковой техники.

Наиболее информативным обнаружителем пустот можно считать тепловизоры, обеспечивающие возможность наблюдения на экране теплового (в инфракрасном диапазоне) изображения обследуемого участка стены. При этом границы пустот очерчиваются достаточно чётко, даже если разница

температур воздушной полости и материала стены составляет всего доли градуса. Инфракрасную камеру тепловизора для наблюдения изображения объекта обычно размещают перед ним на треноге (штативе).

Принцип действия поисковых металлодетекторов (металлоискателей) основан на анализе характеристик сигнала, наводимого в измерительной катушке прибора вихревыми токами, создаваемыми в исследуемом объекте магнитным полем поисковой катушки металлодетектора. Для поиска средств НСИ обычно применяются ручные металлодетекторы. Поиск осуществляется последовательным перемещением металлодетектора над поверхностью исследуемого предмета или элемента конструкции со скоростью около полуметра в секунду. Об обнаружении ферромагнитного объекта свидетельствует появление звукового или светового сигнала. В некоторых типах металлодетекторов, например, в приборе УНИСКАН 7215, решена задача классификации обнаруженных объектов в зависимости от материала, из которого они изготовлены [13]. Для повышения надёжности обнаружения средств НСИ рекомендуется предварительно удалить из зоны поиска все металлические или изготовленные с применением ферромагнитных материалов предметы. Естественно, что поиск таким прибором средств НСИ, установленных, например, рядом с сейфом или радиатором системы отопления невозможен.

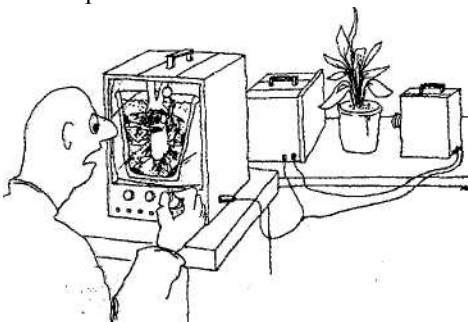
Приборы нелинейной радиолокации считаются некоторыми специалистами единственным техническим средством, обеспечивающим почти стопроцентную гарантию выявления в помещении скрытых радиоэлектронных устройств [3]. Это можно считать справедливым, если выполняется ряд условий, главным из которых является отсутствие в зоне поиска других радиоэлектронных средств. Вместе с тем, это условие не всегда выполнимо, особенно в случаях проверки помещений со стационарно установленной радиоэлектронной аппаратурой или проверки элементов ограждающих помещений конструкций, на внешней стороне которых размещены электронные приборы. Другим важным условием надёжной работы приборов нелинейной радиолокации является их электромагнитная совместимость с другими электронными системами, работающими вблизи проверяемых помещений. Выполнение этого условия также не всегда возможно, особенно в сложной радиоэлектронной обстановке больших городов, промышленных и научных центров.

Большинство приборов нелинейной радиолокации конструктивно состоит из переносного блока приёмопередатчика, связанного кабелями с антенной системой, которая размещена на конце удерживаемой в руках штанги. Метод поиска средств НСИ с помощью такого прибора аналогичен применению ручного металлодетектора: из зоны поиска предварительно удаляются радиоэлектронная аппаратура и все предметы, содержащие радиоэлектронные компоненты, после чего головка антенной системы

прибора вручную перемещается над поверхностью обследуемого предмета или элемента конструкции помещения. На наличие в зоне поиска скрытого электронного устройства указывает характерный звуковой сигнал и показания светового индикатора. Перемещение головки антенной системы над исследуемой поверхностью стены или предмета рекомендуется осуществлять *по* спирали, то есть круговыми движениями с одновременным продольным перемещением центра круговых движений вдоль поверхности стены. Для исключения возможных пропусков участков исследуемой поверхности продольные перемещения головки следует проводить не хаотично, а по определённому закону, например, построчно справа налево или зигзагом. Скорость перемещения во многом зависит от внешних условий. В благоприятных условиях производительность поиска обычно составляет около двух квадратных метров обследуемой поверхности в секунду.

Основной проблемой поиска с использованием приборов нелинейной радиолокации являются ложные срабатывания, вызываемые обычно коррозионными металлическими конструкциями и местами соединения двух различных металлов. Распознавание ложных срабатываний - задача оператора, работающего с прибором. Правильное решение этой задачи требует от оператора определённых навыков и опыта проведения поисковых работ. В простых и относительно дешёвых приборах сигнал, отражённый от скрытого электронного устройства, обычно распознаётся по затуханию в наушниках демодулированного шумового сигнала при приближении антенной системы к месту расположения устройства. Об обнаружении коррозионной конструкции обычно свидетельствует характерный треск в наушниках, возникающий при вибрационном физическом воздействии: постукивании по стене резиновым молотком или кулаком в месте обнаружения сигнала [14].

Проблема распознавания ложных срабатываний во многом облегчается в приборах, обеспечивающих анализ отражённого сигнала одновременно на второй и третьей гармониках частоты зондирующего сигнала. Оператор делает вывод об обнаружении электронного устройства по превышению уровня сигнала, принятого на второй гармонике частоты передатчика, над уровнем сигнала, принятого на её третьей гармонике.



Для расширения зоны обнаружения прибора перед началом его применения обычно устанавливают максимальную мощность передатчика,

максимальное усиление или чувствительность его приёмного тракта. При обнаружении отклика на зондирующий сигнал мощность излучения, усиление или чувствительность приёмного тракта последовательно снижают для более точной локализации источника отражённого сигнала. Снижением мощности передатчика, чувствительности приёмника и усиления сигнала в его тракте можно заметно снизить дальность и глубину обнаружения прибором электронных компонентов. Используя эту особенность, иногда удаётся применять прибор для поиска средств НСИ даже в таких условиях, когда нет возможности удалить электронные приборы от противоположной стороны исследуемой стены. Производительность поиска при этом может снизиться в три-пять раз.

Необходимость предварительного удаления из зоны поиска прибором нелинейной радиолокации всех электронных устройств является причиной того, что обычно применение этого прибора возможно лишь после проведения визуального осмотра помещения. Четкие, однозначные указания индикаторов прибора на обнаружение объекта с электронными компонентами требует от поисковой бригады принятия решения на вскрытие обследованного предмета или элемента конструкции. Право на принятие такого решения может оставаться и руководителем предприятия. Во многих случаях перед принятием такого решения проводится дополнительное обследование скрытого в предмете или стене объекта с помощью флуороскопа или рентгенотелевизионного устройства.

Необходимым условием для применения флуороскопов и рентгенотелевизионных устройств является доступность обеих сторон исследуемого участка стены, элемента конструкции или предмета. Для работы этой аппаратуры необходим рентгеновский излучатель, в качестве которого используется портативный рентгеновский аппарат или радионуклидный источник гамма-излучения. Рентгеновский излучатель и устройство визуализации (рентгено-телевизионный преобразователь) размещают с разных сторон исследуемого участка стены или предмета. Светотеневая картина внутренней структуры просвечиваемого участка наблюдается оператором через окуляр флуороскопа или на экране телевизионного видеоконтрольного устройства. Возможности некоторых современных рентгенотелевизионных комплексов расширены за счёт включения в их состав ПЭВМ или электронных модулей обработки и записи изображения. Сопряжение с ПЭВМ позволяет осуществлять автоматическое сравнение изображений внутренней структуры предметов с хранящимися в базе данных их эталонными изображениями. Для работы с некоторыми типами этой аппаратуры требуется не менее двух операторов.

Общая методика работы с этим видом аппаратуры включает:

- тщательно развёртывание её компонентов относительно исследуемого участка стены или предмета (исследуемый участок должен находиться в зоне

действия прямого пучка излучения, экран устройства визуализации должен быть размещён вплотную к исследуемому предмету);

- выполнение необходимых мер безопасности (правильное размещение оператора, удаление посторонних лиц из зоны действия прямого и рассеянного излучения, работа с минимально необходимой мощностью рентгеновского излучателя и т. д.);

- правильную интерпретацию наблюдаемого изображения, сравнение его с эталонным, при необходимости - запись наблюдаемого изображения (архивацию) и обработку;

- свёртывание аппаратуры или перемещение её компонентов для исследования следующего предмета или участка стены.

В вызывающих сомнения случаях для правильной интерпретации наблюдаемого изображения следует, по возможности, изменить ракурс наблюдения. С этой целью необходимо развернуть предмет в поле действия пучка излучения или изменить угол облучения и наблюдения предмета путём перестановки основных компонентов аппаратуры. Обнаружение элементов электронных устройств на изображении внутренней структуры предмета, который заведомо не должен их содержать (цветочный горшок, пепельница, урна), указывает на наличие в предмете встроенного средства НСИ.

### 2.3. Проверка линий и оборудования проводных коммуникаций.

Широкое распространение средств НСИ, использующих проводные линии для своего электропитания, снятия информации или её передачи, а также удобство маскировки этих средств в разнообразном установленном на проводных линиях оборудовании и подключаемых устройствах требуют от членов поисковой бригады особого внимания к проверке линий и оборудования проводных коммуникаций. Основными видами поисковых работ в ходе проверки являются *визуальный осмотр* линий и оборудования проводных коммуникаций, *поиск сигналов* средств НСИ в проводных и кабельных линиях с помощью специальной поисковой аппаратуры, а также *проверка линий с помощью специальной аппаратуры на наличие подключённых средств НСИ (несанкционированных подключений)*.

Общая методика проверки одинакова для линий и оборудования различного назначения. Проверка осуществляется в соответствии с имеющимися схемами прокладки и монтажа линий, в ходе проверки составленные ранее схемы уточняются. Проверку сложной сети, имеющей большое количество отводов, обычно проводят по отдельным её участкам.



Некоторые отличия, связанные с обеспечением электробезопасности членов поисковой бригады, присущи поиску средств НСИ в линиях и оборудовании силовой и осветительной электросети. Незначительные особенности проведения поисковых работ в линиях и оборудовании других проводных коммуникаций могут быть связаны с применением различных типов специальной поисковой аппаратуры.

Проверке подлежат оборудование, проводные и кабельные линии:

- силовой и осветительной электросети;
- офисной и абонентской телефонной сети;
- селекторной связи;
- радиотрансляционной сети;
- пожарной и охранной сигнализации;
- системы часофикации;
- невыясненного назначения.

При проверке линий и оборудования *силовой и осветительной электросети* целесообразно схему обследуемой сети разделить на несколько отдельных участков, каждый из которых сравнительно легко может быть отключён от источника питающего напряжения. Последующий осмотр линий и оборудования следует проводить последовательно по каждому из этих участков.

Перед *визуальным осмотром* каждый проверяемый участок сети целесообразно обесточить. Принимаются меры для исключения случайной подачи на него напряжения: вывинчиваются пробки, между контактами рубильника, магнитного пускателя вставляется диэлектрическая прокладка, на рубильник и автоматы питания вывешиваются плакаты «Не включать, работают люди!», отсоединённый на распределительном щите провод изолируется т.п. При невозможности обесточить участок, а также в случаях, когда обесточивание нежелательно по соображениям конспирации, работы должны проводиться не менее чем двумя членами поисковой бригады, имеющими допуск к работе на электроустановках с напряжением до 1000 вольт.

При проведении визуального осмотра рекомендуется придерживаться следующей последовательности работ:

- перед осмотром каждого электроустановочного, коммутационного изделия, другого оборудования коммуникаций или участка проводных (кабельных) линий с открытыми для доступа токоведущими частями проверяется отсутствие на них напряжения с помощью тестера, другого измерительного или индикаторного прибора;
- проверяется целостность нанесённых в ходе предыдущих осмотров скрытых меток и пломб, установленных на крышках оборудования и других его съёмных элементах; по инвентарным номерам и скрытым меткам

убеждаются в отсутствии новых или подменённых элементов оборудования;

- в случае подозрений на вскрытие изделия, элемента, а также при обнаружении новых, недавно установленных изделий эти изделия, элементы оборудования вскрываются, разбираются и осматриваются; при осмотре следует убедиться в стандартном расположении элементов внутреннего устройства, отсутствии под крышкой посторонних предметов, новых деталей или элементов неясного назначения, подключений посторонних проводников к токоведущим частям;

- выявленные подозрительные детали и элементы тщательно осматриваются для установления их истинного назначения; при осмотре обращается внимание на отсутствие признаков их сложного, нестандартного внутреннего устройства, отсутствие проводников, небольших отверстий, которые могут служить признаком наличия скрытого микрофона; при необходимости для исследования привлекаются специальные технические средства неразрушающего контроля;

- осматриваются места установки изделий и оборудования: электрощиты, распределительные и установочные коробки, боксы, установочные ниши; особое внимание уделяется осмотру подходящих кабелей, проводов и элементов их скрытой подводки: кабельных каналов, электротехнических труб, металлорукавов, гофрошлангов, пазов, штроб и отверстий в стене и других ограждающих конструкциях; проводаи кабели в ходе осмотра следует вытянуть из закладных труб (кабельных каналов) на максимальную длину, чтобы убедиться в отсутствии несанкционированных подключений к проводам;

- осмотром убеждаются в отсутствии посторонних предметов и подключений на всём протяжении открытых участков прокладки кабелей и проводных линий, а также на участках их прокладки в наружных кабельных каналах (коробах), с этой целью крышки кабельных каналов на время осмотра должны быть демонтированы.

Помимо щитов, распределительных коробок, розеток, выключателей, электропатронов и других установочных изделий осмотру внутри (с разборкой) подлежат все подключаемые к силовой и осветительной сети разветвители, переходники и потребители электроэнергии, не относящиеся к сложным электронным приборам: удлинители, тройники, люстры, бра, люминисцентные светильники, настольные лампы, кондиционеры, вентиляторы, нагревательные приборы и т. д. Не следует забывать также о необходимости разборки и осмотра сетевых штепсельных вилок потребителей электроэнергии.

Для поиска сигналов средств НСИ в проводных кабельных линиях с помощью специальной поисковой аппаратуры все осветительные, бытовые приборы и другие потребители электроэнергии в проверяемом помещении

должны быть подключены к электросети и приведены в рабочее состояние (включены). Тем самым осуществляется перевод в рабочее состояние возможно внедрённых в эти приборы и устройства средств НСИ. Наличие сигналов средств НСИ проверяется отдельно в каждой фазе систем силовой и осветительной электросети. Для этого поисковый прибор с помощью входящих в его комплектацию специальных щупов (кабелей) поочерёдно подключается к каждой из фаз проверяемой системы.

В проверяемом помещении создаётся требуемый для активизации средств НСИ с акустопуском и дальнейшей работы поискового прибора *звуковой фон* (например, от кассетного плеера, магнитолы или настроенного на волну • широкополосной радиостанции радиоприёмника). Напомним здесь ещё раз о том, что создаваемый в помещении звуковой фон является не только источником необходимой для работы многих поисковых приборов «звуковой обратной связи», но и служит для маскировки шумов и звуков, производимых в ходе работ членами поисковой бригады. В этой связи рекомендуется создавать звуковой фон, уместный для ситуации скрытой проверки помещения, сразу с началом проведения визуального осмотра ограждающих конструкций, мебели и других предметов интерьера помещения. Таким звуковым фоном может быть не только и не столько музыка, сколько воспроизведение предварительно сделанной записи производственных шумов, доклада, делового семинара, занятий по совершенствованию профессиональной подготовки, не вызывающих насторожённости и подозрений у подслушивающего противника. Длительность подготовленных записей не должна быть меньше запланированной продолжительности поисковых и исследовательских работ.

Методика дальнейших действий определяется типом используемого для выявления сигналов средств НСИ поискового прибора. Как правило, все приборы такого назначения имеют высокочувствительный малошумящий усилитель низкой частоты, позволяющий обнаруживать в линии сигналы звукового диапазона частот, и перестраиваемый приёмник высокочастотных электрических сигналов. Поиск высокочастотных сигналов осуществляется вручную или автоматически путём перестройки приемника по частоте. В процессе поиска обеспечивается индикация уровней обнаруженных сигналов, демодуляция сигналов и их слуховой контроль.

При наличии в линии сигналов подслушивающего устройства через наушник прибора на выходе приёмника можно услышать акустический фон обследуемого помещения, озвученного магнитолой (радиоприёмником), или соседних помещений. Прослушивание слабого акустического фона помещения на выходе высокочувствительного усилителя низкой частоты обычно говорит о наличии в помещении устройства, обладающего «микрофонным» эффектом. Обнаружение в линии мощного высокочастотного сигнала может свидетельствовать о применении противником аппаратуры

высокочастотного навязывания для прослушивания помещения.

Уточнить местоположение подслушивающего устройства, сигналы которого обнаружены в линии, можно двумя способами: последовательным перемещением вдоль линии места подключения прибора и поочерёдным отключением от сети потребителей электроэнергии. Если громкость обнаруженных сигналов возрастает при изменении места подключения прибора (например, при включении щупов прибора в разные сетевые розетки), это означает, что мы приближаемся к месту подключения средства НСИ. В случае, когда таким способом не удаётся локализовать место установки средства НСИ, следует попытаться поочерёдным отключением бытовых приборов и других потребителей определить, какой из них является «носителем» подслушивающего устройства. Обнаружение такого потребителя должно побудить поисковую бригаду к его тщательному исследованию с задачей найти само это устройство. Следует помнить, что часть сетевых розеток может быть подключена к электрической сети через трансформаторы, не пропускающие сигналы средств НСИ. В таких цепях поиск сигналов необходимо проводить, включая прибор в розетки, подключённые как к первичной, так и к вторичной обмотке трансформатора.

В некоторых случаях поиску сигналов средств НСИ мешает высокий уровень низкочастотного шума в проверяемой линии. Источником такого шума могут быть регуляторы освещённости, дефектные люминисцентные лампы или блоки питания устройств бытового назначения. Для снижения уровня шума следует, не отключая шумящей цепи от проверяемой линии, вывести регулятор освещённости на максимум или удалить шумящую лампу. «Шумящий» блок питания можно определить последовательным отключением от сети потребителей электроэнергии. Найденный источник шума подвергается тщательной проверке на наличие внедрённого средства НСИ.

Убедившись в отсутствии информативных сигналов в линиях силовой и осветительной электросети, переходят к *проверке* линий *на наличие подключённых средств НСИ (несанкционированных подключений)*. Проверка осуществляется с использованием нелинейного детектора (локатора) проводных коммуникаций. Принцип действия такого прибора основан на подаче в линию зондирующего сигнала и регистрации его гармоник, возникающих в нелинейных элементах подключённого к линии средства НСИ. Методика работы прибором заключается в следующем:

- проверяемый участок сети отключается от источника питающего напряжения и всех легальных потребителей электроэнергии (вилки электроприборов отключаются от розеток, из люстр и бра вывинчиваются все электрические лампы, выключатели освещения должны оставаться во включённом состоянии);
- прибор подключается к линии в начале проверяемого участка сети,

к противоположному концу линии подключается испытательная нагрузка;

- прибором в линию подаётся зондирующий сигнал, оператором визуально, по наличию искажений эталонного изображения на экране прибора определяется присутствие высших гармоник в принимаемом сигнале, свидетельствующее о факте нелегального подключения к линии; по виду искажений эталонного изображения можно судить о характере подключённого к линии устройства.

Для уточнения места подключения можно расчленив проверенный участок сети на несколько частей и в каждой из них повторить описанные выше процедуры. Окончательное определение места подключения и непосредственное обнаружение подключённого устройства осуществляются путём повторного визуального осмотра участка линии, на котором найдено нелегальное подключение. При необходимости поиск подключённого устройства может быть проведён с помощью прибора нелинейной радиолокации. Проверку линий проводят до тех пор, когда для всех участков силовой и осветительной электросети на экране нелинейного детектора (локатора) проводных линий будет получено неискажённое эталонное изображение.

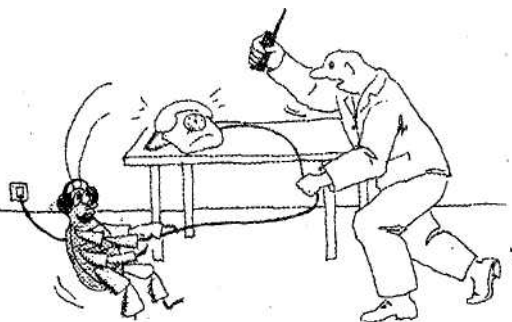
Проверка *офисной и абонентской телефонной сети* осуществляется в той же последовательности. Визуальный осмотр линий и оборудования заключается в поиске несанкционированных подключений к телефонным проводам телефонному оборудованию, поиске посторонних предметов и вызывающих подозрение деталей телефонных аппаратах, вилках, розетках, распределительных коробках, оборудовании офисной АТС, в телефонном шкафу.

Опыт показывает, что до семидесяти процентов средств НСИ, обнаруживаемых в ходе проведения поисковых работ, составляют средства, непосредственно снимающие информацию с телефонной линии, либо использующие телефонную линию для передачи информации, перехваченной другим способом. Во многих случаях используются комбинированные средства НСИ, осуществляющие перехват телефонных переговоров при снятой телефонной трубке, а в паузах между ними - акустической информации из помещения. Следует помнить, что устройства бесконтактного (индуктивного) съёма информации с телефонных линий на сегодня практически не обнаруживаются ни одним типом поисковых приборов. По этой причине визуальный осмотр телефонных аппаратов, другого телефонного оборудования самих телефонных линий должен проводиться с предельной тщательностью.

При вскрытии телефонных аппаратов следует искать прежде всего нестандартные или чем-либо выделяющиеся, наспех установленные элементы



1 В случае невозможности или нежелательности отключений телефонных линий от АТС можно использовать другие типы приборов, специально разработанные для анализа телефонных линий. Так, телефонное проверочное



устройство ТПУ-6 без отключения телефонных линий от АТС определяет наличие сигнала высокочастотного навязывания, а также последовательно и параллельно подключенных к линии и питающихся от неё средств НСИ. Выявление этим прибором высокоомных и конденсаторных подключений к линии всё же требует отсоединения линии от АТС. Методика работы с этим прибором состоит в его подключении в линию между телефонным аппаратом и телефонной розеткой, переключении режимов прибора и сравнении отображаемых на дисплее результатов измерений с допустимыми значениями параметров свободной от средств НСИ линии.

Анализатор телефонных линий 8ЕБ8Р-18/Т, как утверждают разработчики прибора, без отключения линии от АТС обнаруживает любые гальванически подключённые средства НСИ в автоматическом режиме, что предельно упрощает работу оператора с этим прибором: достаточно подсоединить его к линии и телефонному аппарату и включить питание прибора. Оба прибора позволяют с помощью подключаемых головных телефонов проверять линии на наличие в них низкочастотных сигналов.

У проверенных на отсутствие средств НСИ телефонных линий целесообразно провести измерение их параметров: активного и реактивного сопротивлений, ёмкости и индуктивности. Результаты измерений для двух состояний каждой линии (разомкнутого и замкнутого накоротко) рекомендуется занести в специальную таблицу. Целесообразно также после подключения линии к АТС телефонному аппарату зафиксировать в таблице величину напряжений в линии при поднятой и опущенной на рычаг аппарата трубке. При последующем контроле состояния линий эти данные помогут установить факт и характер произошедших на линиях изменений.

При проверке линий и оборудования систем селекторной связи, радиотрансляционной сети, пожарной и охранной сигнализации, системы часофикации и других проводных систем применяется та же методика поисковых работ, что была рассмотрена выше. Остановимся здесь лишь на

некоторых особенностях проверки проводных линий неизвестного назначения. Как правило, такие линии всегда обнаруживаются в ходе проведения визуального осмотра проверяемого помещения, особенно если оно находится в здании старой постройки.

Эти линии могут быть использованы противником для электропитания средств НСИ, дистанционного управления их включением и выключением, передачи перехваченной средствами НСИ информации, снятия наведённых информативных сигналов. Рекомендуется следовать ЦЖП порядок проверки линий неизвестного назначения:

- визуальным осмотром проводов следует проследить трассу прокладки неизвестной линии для выявления всех имеющихся подключений к линии и её возможного назначения;

- с помощью тестера или индикатора напряжения убеждаются в отсутствии опасного напряжения на проводах линии; в случае обнаружения нескольких неизвестных линий или многопроводного кабеля неизвестного назначения измерения следует провести для всех пар, которые могут быть составлены из проводников, входящих в состав обнаруженных линий и кабеля;

- с помощью прибора проверки проводных линий необходимо убедиться в отсутствии в линии низкочастотных и высокочастотных сигналов; в многопроводном кабеле поиск сигналов следует провести во всех возможных парных комбинациях имеющихся проводников, а также в линиях, образованных каждым из проводников и заземлением;

- подключением нелинейного детектора (локатора) проводных линий проверяют все возможные пары из имеющихся проводников на наличие подключённых средств НСИ, особое внимание при этом обращается на проверку пар, находящихся под напряжением, так как они могут использоваться для электропитания средств НСИ.

Следует помнить, что в проводах, проложенных параллельно телефонной линии, могут наводиться сигналы, перехват которых позволит противнику подслушивать ведущиеся телефонные переговоры. Поэтому следует пометить и зафиксировать в документах осмотра все линии невыясненного назначения для их последующего демонтажа.

В заключение отметим, что для повышения надёжности результатов поиска желательно предпринять не одну, а несколько попыток обнаружить сигналы средств НСИ в проводных линиях. Повторные поиски целесообразно проводить с изменением первоначальной последовательности проверки линий различного назначения и через неравные промежутки времени.



## 2.4. Радиомониторинг проверяемых помещений, локализация радиоизлучающих средств негласного съёма информации.

Для проведения радиомониторинга проверяемого помещения в нём развёртывается пункт радиоконтроля с комплектом необходимой радиоприёмной и анализирующей аппаратуры. Основными задачами радиомониторинга на этапе непосредственного проведения комплексной специальной проверки помещений являются выявление радиоизлучений средств НСИ и определение их местоположения. Кроме того, радиомониторинг позволяет обнаружить факты преднамеренного высокочастотного облучения помещений специальными генераторами, а также выявить информативные побочные электромагнитные излучения работающих в помещении средств оргтехники.

Для надёжного выявления радиоизлучающих средств НСИ радиомониторинг должен проводиться в условиях максимальной активизации этих средств: выполнения мер, предусмотренных легендой, для активизации разведки противника; озвучки помещения воспроизведением записи «деловых переговоров»; снятия трубок телефонных аппаратов для перевода телефонных линий в режим «занято»; включения всех источников освещения, бытовых приборов и средств оргтехники. Вместе с тем, следует, по возможности, избегать ведения радиомониторинга при одновременной работе радиоизлучающих видов поисковой и исследовательской аппаратуры, особенно такой, как приборы нелинейной радиолокации.

В случае проведения предварительного сбора данных радиоэлектронной обстановки и их анализа оператор пункта радиоконтроля уже должен располагать картой занятости радиоэфира, базой данных выявленных и идентифицированных радиосигналов и списком частот «подозрительных» радиоизлучений. Если же эта работа по каким-либо причинам не была проведена в ходе подготовительного этапа, её придётся выполнять уже в ходе непосредственного проведения проверки помещения в соответствии с методикой, изложенной в разделе 1.7.

Располагая составленным ранее картой занятости радиоэфира, базой данных выявленных и идентифицированных радиосигналов и списком частот «подозрительных» радиоизлучений, оператор пункта радиоконтроля должен снять текущую панораму загрузки радиодиапазона и сверить принимаемые излучения с имеющейся базой данных. По результатам сверки выявляются, анализируются и идентифицируются новые излучения, пополняется база данных и список частот «подозрительных» радиоизлучений. Такое снятие текущих панорам загрузки в процессе радиомониторинга помещения должно проводиться неоднократно, чтобы снизить вероятность случайного

пропуска излучений, непостоянно присутствующих в эфире: внешнего высокочастотного облучения помещения, сигналов дистанционного управления включением средств НСИ, сигналов периодически излучающих средств НСИ (осуществляющих передачу предварительно накопленной информации) и т. п.

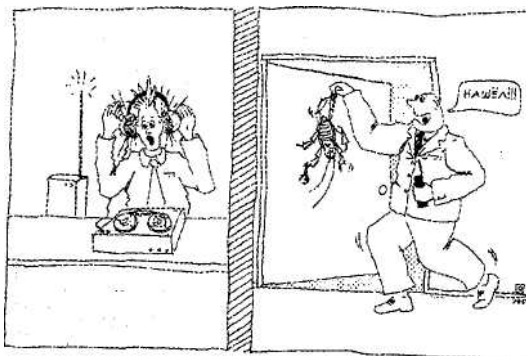
Следует иметь в виду, что иногда сигналы средств НСИ пытаются замаскировать под излучения известных легальных источников. Поэтому при сравнении панорам загрузки радио диапазона, снятых в разное время, следует обращать внимание на все существенные изменения характеристик известных сигналов: внезапное возрастание уровня сигнала, расширение его спектра или появление сигнала вне обычного для него расписания. При обнаружении таких изменений необходимо взять сигнал на контроль, провести его ручной анализ и в случае подозрений занести его в список частот «подозрительных» радиоизлучений.

Дальнейшая работа оператора заключается в тестировании и анализе «подозрительных» радиоизлучений на принадлежность к излучениям средств НСИ и ПЭМИ средств оргтехники из проверяемых помещений. Методика тестирования во многом определяется типом используемой аппаратуры. В большинстве автоматизированных программно-аппаратных комплексов тестирование на принадлежность излучений к средствам НСИ проводится автоматически, путём сравнения характеристик «подозрительного» излучения с заложенными в программу признаками излучений средств НСИ.

Поисковое

программное обеспечение современных комплексов позволяет проверять излучения сразу по нескольким критериям.

Так, универсальное программное обеспечение ФИЛИН реализует до восьми одновременно используемых алгоритмов обнаружения средств НСИ.



Наиболее достоверным признаком работы подслушивающего радиоизлучающего устройства считается присутствие признаков модуляции тестируемого излучения звуками проверяемого помещения. Для повышения надёжности обнаружения таких признаков практически во всех программно-аппаратных комплексах реализован алгоритм проверки корреляции между модулирующей функцией «подозрительного» сигнала и специально

излучаемым аппаратурой акустическим тестовым сигналом. Однако такой метод тестирования обычно демаскирует факт проведения проверки, поэтому мы рекомендуем использовать режим бесшумной корреляции, обеспечиваемый некоторыми современными программно-аппаратными комплексами. Использование этого режима тем более оправдано, поскольку проверяемое помещение/уже озвучено магнитолой или радиоприёмником.

Завершающим этапом работы оператора с источником излучения, идентифицированным как средство НСИ, является уточнение его местонахождения и визуальное обнаружение. Визуально обнаруженное средство НСИ изымается, нейтрализуется или сохраняется в рабочем состоянии в соответствии с ранее принятым вариантом действий.

Локализация источников излучений, идентифицированных комплексами как средства НСИ, осуществляется в большинстве комплексов по команде оператора методом триангуляционной акустической локации в двухмерном или трёхмерном пространстве. Перед этим источники зондирующих сигналов (обычно - акустические колонки) размещают в помещении таким образом, чтобы обеспечить необходимую базу пеленгации, и осуществляют пространственную привязку источников к плану помещения путём ввода параметров помещения и координат источников в управляющую программу.

Неоднозначность результатов акустической локации может быть следствием переотражений зондирующего сигнала предметами обстановки помещения или воздействия посторонних шумов. Обычно неоднозначность результатов исчезает, если звуковые колонки расположить иначе и соблюдать во время локации в помещении тишину. Следует помнить, что акустическая локация выявляет местоположение микрофона подслушивающего устройства, а не его радиопередатчика. Поэтому, если визуальный осмотр указанного аппаратурой места не позволяет обнаружить подслушивающее устройство целиком, следует искать спрятанный микрофон и идущие от него к основной части средства НСИ провода.

Характерные звуки зондирующих сигналов обычно позволяют противнику установить факт обнаружения подслушивающего устройства. Для повышения скрытности поиска можно воспользоваться общеизвестным методом локализации источника излучения по возрастанию уровня принимаемого сигнала. Проще всего этот метод реализуется с помощью детекторов (индикаторов) поля и ручных частотомеров с индикаторами уровней принимаемых сигналов. Для повышения точности местоуказания чувствительность этих приборов постепенно, по мере приближения к источнику излучения снижают.

Иногда показания детектора поля не позволяют точно определить максимум излучения или дают сразу несколько максимумов в небольшой области пространства. Одной из наиболее вероятных причин таких показаний может быть размещение средства НСИ вблизи объёмной металлической

конструкции, искажающей структуру электромагнитного поля. Зная об этом, следует с особой тщательностью осмотреть сейфы, металлические шкафы, стеллажи и другие металлические конструкции в данной части помещения.

Другой возможной причиной неявных показаний детектора поля может быть применение противником подслушивающего устройства, радиопередатчик которого вынесен за пределы проверяемого помещения. В этом случае, скорее всего, придётся воспользоваться возможностями акустической локации для определения местоположения микрофона, несмотря на недостатки этого метода.

Наконец, довольно распространённой причиной нечёткой работы детекторов поля и ручных частотомеров является высокий уровень внешних электромагнитных полей в районе проверяемого помещения. Устранить эту причину полностью обычно не удаётся. Можно попытаться выключить возможные источники радиоизлучений в соседних помещениях и попросить сотрудников предприятия на время не пользоваться услугами сотовых систем связи. Однако и в этом случае лучше всего воспользоваться возможностями современных программно-аппаратных комплексов по определению местонахождения средств НСИ методом акустической локации.

Указания индикатора поля или результатов акустической локации на какой-либо бытовой, осветительный прибор или средство оргтехники, как на искомый источник излучения средства НСИ, чаще всего говорят о том, что в данный прибор внедрено радиоизлучающее подслушивающее устройство. В этом случае данный прибор должен быть отключён, разобран и тщательно осмотрен.

Иногда в процессе радиомониторинга помещения удаётся обнаружить слабое излучение, непохожее на излучение средства НСИ, но имеющее признаки модуляции звуками проверяемого помещения. Это излучение может оказаться побочным электромагнитным излучением работающих в помещении средств оргтехники или бытовых приборов. Для выявления источника ПЭМИ рекомендуется последовательно отключать от сети работающие средства до полного исчезновения «подозрительного» сигнала. Уверенность в том, что в процессе поиска было обнаружено ПЭМИ прибора, а не излучение средства НСИ, может дать тщательный визуальный осмотр прибора с его полной разборкой и проведение специального дополнительного исследования данного прибора на ПЭМИ. Естественно, что все факты обнаружения таких «радиопередающих» приборов должны найти отражение в отчёте о проведённой проверке для принятия решения руководством предприятия о возможности их дальнейшего использования.

Несмотря на то, что в характеристиках некоторых программно-аппаратных комплексов фирмами-изготовителями заявлено автоматическое обнаружение радиомикрофонов с цифровым закрытием передаваемой информации, в большинстве случаев идентификация таких средств НСИ по их радиоизлучениям остаётся прерогативой оператора.

^5<sup>шп</sup> в ИшениядостовфностиИдентификации\|Б\| рекомендуем использовать метод сравнения уровней «подозрительного» сигнала, принятого в проверяемом помещении и вне его. В случае превышения уровня принимаемого в помещении излучения над уровнем того же сигнала, принятого вне помещения, можно говорить о том, что источник излучения находится где-то рядом, скорее всего, является установленным в помещении средством НСИ. Практическая реализация этого метода возможна либо перемещением антенны радиоприёмника из помещения и обратно, либо развёртыванием в составе комплекса двух переключаемых идентичных антенн (внутри помещения и вне его), либо использованием переносного радиоприёмника, имеющего чувствительный индикатор уровня принимаемого сигнала. Следует иметь в виду, что иногда для чёткой фиксации изменения уровня принимаемого сигнала может потребоваться удаление точки внешнего приёма от проверяемого помещения на несколько десятков или даже сотню метров.

Как правило, ручного анализа и идентификации оператором требуют излучения средств НСИ, в которых применяются нетрадиционные виды модуляции, например, амплитудная модуляция с подавленной несущей или модуляция с использованием поднесущих частот. Широкие возможности современных программно-аппаратных комплексов по детальному ручному анализу спектрограмм, фонограмм, осциллограмм, корреляционных функций и других характеристик принимаемых сигналов позволяют оператору довольно легко решать подобные задачи.

В качестве эффективного метода идентификации принимаемых сигналов можно рекомендовать сравнение характеристик исследуемого сигнала с образцами хранящихся в базе данных характеристик излучений различных средств НСИ. Пополнение такой базы данных - одна из задач, попутно решаемых в ходе проверки специалистами поисковой бригады. Вместе с тем, проблемой остаётся распознавание средства НСИ в случае использования противником средств со скачкообразным изменением несущей частоты, шумоподобными сигналами или сигналами со сверхширокополосной частотной модуляцией. К счастью, такие средства НСИ очень редко применяются криминальными структурами, оставаясь «экзотическим оружием» спецслужб.

Тем не менее, и такие устройства в большинстве случаев могут быть обнаружены довольно простым набором поисковых средств. Вначале следует убедиться, что источник «подозрительного» сигнала находится в самом помещении, а не за его пределами. Для этого следует использовать описанный выше метод сравнения уровней «подозрительного» сигнала в проверяемом помещении и вне его. Лучше всего для этой цели подойдёт переносный сканирующий радиоприёмник с индикатором уровня принимаемого сигнала. В случае подтверждения подозрений дальнейший поиск источника сигнала в помещении проводится с помощью детектора (индикатора) поля,

реагирующего на любой источник излучения вне зависимости от вида модуляции сигнала или изменения его несущей частоты. Заключительной поисковой операцией, как и в других случаях, будет визуальный осмотр места, указанного детектором поля.

В последнее время всё чаще для получения необходимой противнику информации применяются скрыто установленные видеокамеры. Существует специальная аппаратура (IRIS VCF-2000), автоматически обнаруживающая работающие видеокамеры по их собственному побочному радиоизлучению. Выявление такого излучения обычными сканирующими радиоприёмниками в процессе радиомониторинга помещения весьма проблематично ввиду очень слабого уровня сигнала. Вместе с тем, обнаружение излучений видеокамер, передающих видеoinформацию по радиоканалу, обычно достаточно просто осуществляется по характерным признакам, присущим видеосигналу: специфическому спектру, наличию синхронизирующих импульсов в осциллограмме сигнала и др. Некоторые современные программно-аппаратные комплексы, например, OSCOR OSC-5000 Deluxe или КРОНА-6000М, обеспечивают автоматическую идентификацию сигналов радиопередающих видеокамер с возможностью просмотра передаваемого видеоизображения.

Для облегчения последующего анализа проведённой работы и составления отчёта необходима регистрация проводимых операций и результатов поиска. Если поисковой аппаратурой не обеспечивается автоматическая регистрация параметров поиска, в процессе радиомониторинга рекомендуется вести регистрационный журнал.

Как правило, в процессе радиомониторинга помещения его объём проверяется на отсутствие инфракрасных каналов передачи информации средствами НСИ. С этой целью используются зонды-детекторы ИК-излучений, входящие в комплект некоторых многофункциональных приборов (ПИРАНЬЯ, OSCOR OSC-5000 и др.). Для выявления ИК-излучения подключённый прибор ИК-зонд поочередно устанавливается в нескольких различных точках помещения в процессе приёма постепенно поворачивается таким образом, чтобы охватить своим полем зрения все направления, откуда может приходиться ИК-сигнал. Наиболее вероятно, что ИК-сигналы средств НСИ излучаются в направлении окон или застеклённых дверей проверяемого помещения, чтобы обеспечить возможность приёма сигналов за его пределами. Поэтому ИК-зондом поискового прибора следует в первую очередь проверить пространство возле каждого окна и застеклённой двери проверяемого помещения.

В некоторых типах поисковых приборов сектор обзора ИК-зонда в азимутальной плоскости достигает 360 градусов, и поворачивать такой зонд в процессе поиска ИК-сигналов необходимости нет. При обнаружении сигналов определить направление на их источник можно путём частичного перекрытия (например, ладонью или газетой) сектора обзора ИК-зонда с

различных направлений до установления факта пропадания сигнала. После определения направления на источник ИК-сигнала дальнейшая локализация его местонахождения осуществляется путём визуального осмотра размещённых в этом направлении элементов ограждающих конструкций и предметов интерьера.

## 2.5. Поиск средств негласного съёма информации, внедрённых в электронные приборы.

Иногда результаты определения местоположения источников информативных сигналов, выявленных в процессе радиомониторинга помещений поиска сигналов в проводных коммуникациях, указывают на средства оргтехники или бытовые приборы, которые по своей элементной базе могут быть отнесены к электронным приборам. В настоящее время к этому классу приборов следует относить не только сложные радиоэлектронные устройства типа ПЭВМ, телефаксов, магнитофонов теле-радиоприёмников, но и менее сложную аппаратуру, в состав которой входят электронные управляющие устройства: переключатели режимов, таймеры, регуляторы мощности и т. п.

Выделение электронных приборов в отдельную категорию предметов, проверяемых в ходе комплексной специальной проверки помещений, связано с тем, что они чрезвычайно удобны для установки в них средств НСИ. Электронные приборы позволяют легко решить проблему электропитания внедрённых средств НСИ, обеспечивают идеальные условия для быстрой установки средств НСИ, камуфлированных под конденсаторы, фильтры, реле и другие стандартные элементы и узлы. Многие электронные приборы сами по себе являются средством приёма, обработки, хранения и передачи конфиденциальной информации. В то же время обнаружение в них средств НСИ затруднено ввиду невозможности или малой эффективности использования некоторых видов специальной поисковой аппаратуры: приборов нелинейной радиолокации, металлодетекторов, решётчатотелевизионных комплексов. Всё это послужило причиной появления особой методики поиска средств НСИ в электронных приборах.

Эта методика включает:

- поиск информативных сигналов на всех входах и выходах прибора, подключаемых к внешним проводным линиям, включая линию электропитания прибора;
- поиск информативных радиоизлучений прибора;
- разборку и визуальный осмотр основных узлов и элементов прибора.

Для поиска внедрённых в электронный прибор средств НСИ этот прибор обычно размещают на отдельном столе. При отсутствии автономного источника питания прибор подключают к электрической сети и включают в обычный для него рабочий режим.

Поиск высокочастотных и высокочастотных информативных сигналов на всех подключаемых к прибору проводных линиях входов и выходов прибора проводится с помощью аппаратуры, применяемой для поиска сигналов в ходе проверки линий и оборудования проводных коммуникаций. Методика поиска сигналов - стандартная и отличается лишь тем, что поиск информативных сигналов в электронном приборе, относясь к средствам приёма, обработки, хранения и передачи конфиденциальной информации, для повышения надёжности результатов необходимо проводить отдельно для каждого рабочего режима проверяемого прибора.

Полномасштабный поиск информативных радиоизлучений прибора включает проверку общего уровня радиоизлучений с помощью детектора поля для обнаружения внедрённых радиопередающих средств НСИ и проверку уровня информативных ПЭМИ прибора. Измерения и количественная оценка спектральных составляющих ПЭМИ относятся к специальным исследованиям и требуют применения специальной аппаратуры (например, комплекса проведения исследований на свч-информативные побочные электромагнитные излучения НАВИГАТОР), поэтому во многих случаях ограничиваются проверкой общего уровня радиоизлучений прибора с помощью детектора (индикатора) поля.

Отсутствие информативных сигналов по результатам проверки проводных входов и выходов прибора, а также его радиоизлучений не является гарантией того, что эти сигналы и радиоизлучения не появятся по сигналу запроса противника или в назначенное им время. Поэтому основным элементом методики поиска средств НСИ, внедрённых в электронный прибор, считается разборка и визуальный осмотр основных узлов и элементов прибора. Перед разборкой прибор обесточивается (отключается от сети). Визуальный осмотр проводится с применением фонарей для подсветки деталей, луп различной кратности увеличения, небольших зрительных приборов. В большинстве случаев не удаётся обойтись и без пинцета с паяльником. Визуальному осмотру помогают нанесённые в ходе предыдущей проверки скрытые метки и скрытая маркировка деталей и узлов прибора.

В ходе осмотра прежде всего должны быть проверены целостность сделанных ранее скрытых меток, соответствие маркировки и номеров узлов, печатных плат прибора его паспорту и старым записям в регистрационном журнале. В ходе осмотра следует искать:

- посторонние предметы, находящиеся (подброшенные, приклеенные, привинченные, вставленные в свободные разъёмы) под кожухом прибора; ;
- не предусмотренные схемой прибора («лишние») подпаянные или



вставленные в свободные разъёмы радиодетали и узлы;

- не предусмотренные схемой прибора перемычки, подпайки к деталям схемы проводников, особенно имеющих второй конец свободным или подсоединённым к выходящим за пределы прибора проводам;

- заметно отличающиеся от стандартных по своим габаритам, цвету, маркировке или её отсутствию детали и узлы;

- следы нефабричной пайки, указывающие на возможность подмены установленной в заводских условиях детали;

- следы поспешной установки или подмены соединительных шлангов и других элементов на разъёмах (перекос, нестандартный или подозрительный внешний вид элемента).

Тщательно осмотрены должны быть все детали и узлы, по своим габаритам способные содержать средство НСИ.

Таковыми деталями,

подменёнными и

противником на

закамуфлированные под

них средства НСИ, могут

быть бумажные,

электролитические или

другие им равные по

объёму конденсаторы,

резисторы большой

мощности, микросхемы,

катушки индуктивности,

подстроечные контуры,

кварцевые резонаторы,

разъёмы, переключатели,

закрытые экранирующим кожухом элементы схемы.

При осмотре таких деталей следует обращать внимание на нетипичность

маркировки или её отсутствие, на нестандартность внешнего вида или

крепления на плате, на наличие подпаянных внешних проводников или изменений

в рисунке печатных проводников на плате в месте нахождения детали, на

наличие в корпусе деталей отверстий, за которыми может скрываться

микрофон подслушивающего устройства.

Для работы скрытого микрофона обычно достаточно небольшого,

диаметром около одного миллиметра отверстия, которое может быть

проделано на стороне детали, обращенной к монтажной плате, и тем самым

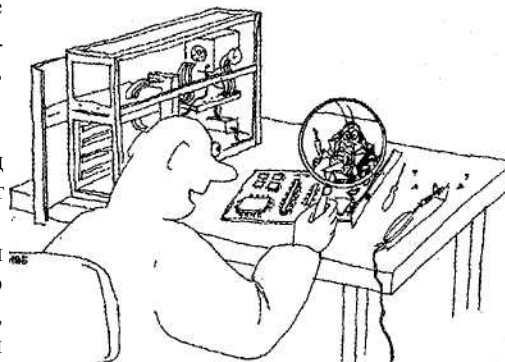
скрыто от поверхностного взгляда. Поэтому рекомендуется, если возможно,

пользоваться для осмотра труднодоступных поверхностей деталей небольшим

зеркалом или выпаять вызывающие сомнения детали для их всестороннего

осмотра. В некоторых случаях может потребоваться проведение осмотра

внутренней структуры подозрительной детали с помощью флуороскопа или



рентгенотелевизионного устройства.

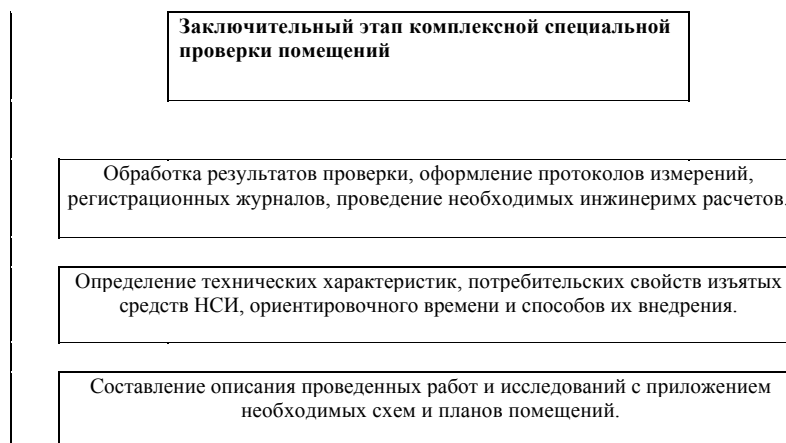
Ускорению и надёжности результатов осмотра способствуют заранее подготовленные электрические и электромонтажные схемы прибора и его составных элементов (отдельных блоков, печатных плат), фотографии монтажа и узлов прибора, сделанные в ходе предыдущей проверки или на другом экземпляре того же прибора, образцы печатных плат и узлов, снятые с другого экземпляра такого же прибора. При наличии фотографий и образцов печатных плат поиск имеющихся в проверяемом приборе отличий осуществляется методом фавнения с эталоном, то есть путём фавнения внешнего вида плат и узлов прибора с имеющимися фотографиями и образцами.

По окончании осмотра проводится выборочная скрытая маркировка отдельных деталей и узлов прибора, устанавливаются скрытые метки на съёмных крышках, элементах крепления печатных плат и узлов, делаются соответствующие памятные записи в регистрационном журнале, прибор собирается, проверяется на работоспособность во всех режимах и опечатывается.

### 3. Заключительный этап комплексной специальной проверки помещений.

Заключительный этап комплексной проверки помещений включает работы, выполняемые, в основном, за пределами предприятия, в помещениях организации, проводившей провфку. Содержание заключительного этапа представлено на схеме 4.

*Схема 4*



Разработка рекомендаций по повышению защищенности проверенных помещений:

составление перечня и схем выявленных технических каналов утечки информации по каждому помещению;

оценка степени существующей *защиты* каждого помещения 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;  
инженерных;  
технических.

составление свободного перечня технических средств и систем, рекомендуемых к установке для защиты информации от утечки по техническим каналам;

разработка предложений по способам использования рекомендуемых технических средств и систем и объединению их в единую комплексную систему защиты информации;

Составление акта проведения комплексной специальной проверки помещений.

Предоставление итоговых и отчетных документов руководителю предприятия для утверждения.

### 3.1. Обработка результатов исследования.

Как бы тщательно ни были проведены подготовительные работы, маловероятно, чтобы удалось обойтись без внесения корректив в программу поиска, сданных на скорую руку заметки памятных записей, фиксирующих уточнение и появление новых задач, последовательность их решения, промежуточные результаты работ и измерений. Поскольку все записи, относящиеся к проведению комплексной специальной проверки помещений, считаются конфиденциальной информацией, их следовало вести в отдельных

учтённых тетрадах. В них же, скорее всего, велись записи, заменявшие переговоры между членами поисковой бригады для скрытия речевых признаков проведения проверки. Поэтому к концу этапа непосредственного проведения проверки на руках у членов бригады обычно остаётся несколько исписанных тетрадей, включающих наспех изготовленные рисунки и схемы, фрагменты переговоров, протоколов измерений, таблиц и другие записи, требующие своего упорядочения.

В этой связи первым шагом в обработке результатов проверки должна быть инвентаризация записей, которые понадобятся для разработки и оформления итоговых и отчётных документов. Она заключается в составлении сводного перечня представляющих ценность записей, схем и таблиц с указанием номеров тетрадей и страниц, где они содержатся.

Следующие шаги могут быть представлены следующим образом:

- оформление регистрационных журналов, включающее упорядочение инвентаризационных записей мебели, оборудования и предметов проверяемых помещений, структуризацию и оформление записей и рисунков оставленных скрытых меток, поставленных печатей и пломб;

- внесение выявленных в ходе проверки уточнений в планы помещений, расстановки мебели, схемы размещения предметов, проводных и инженерных коммуникаций;

- изготовление рисунков и схем, отражающих места и способы установки найденных средств НСИ;

- оформление таблиц, включающих данные измерений;

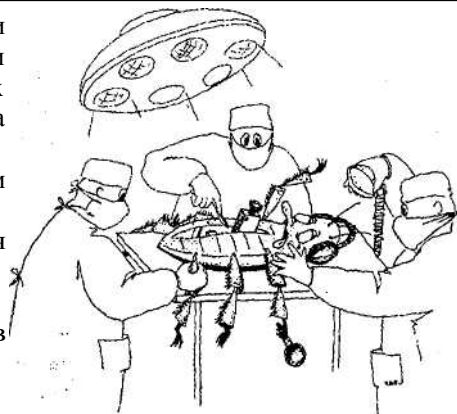
- проведение необходимых инженерно-технических расчётов по результатам измерений:

- оформление протоколов измерений, включающее оформление протоколов, заполнявшихся на заранее заготовленных бланках, распечатку протоколов, составленных автоматизированными графоаммно-аппаратными комплексами в процессе своей работы, сведение в единый документ фрагментов записей и таблиц, составленных в ходе выполнения внезапно возникших, непредусмотренных первоначальным планом задач;

- уточнение данных об использованных в процессе поисковых и исследовательских работ приборах, оборудовании, режимах и условиях их работы.

Важным элементом этого этапа является обобщение опыта поисковых и исследовательских работ, накопленного за время проведённой проверки. С этой целью анализируются выявившиеся в ходе работ недостатки использовавшихся методик и приборов, оценивается правдоподобность и пригодность выбранных методов работы активизации средств НСИ, результативность мер по сокращению общего времени проведения проверки, целесообразность внедрения новых приёмов работ, обобщаются полученные

полученные в ходе проверки новые данные о способах и средствах, применяемых противником для перехвата **конфиденциальной** информации. По результатам радиомониторинга помещений пополняются базы данных идентифицированных радиосигналов и сигналов средств НСИ.



По материалам проведённой проверки рекомендуется подготовить сведения, характеризующие трудозатраты на выполнение отдельных видов поисковых и исследовательских работ, рассчитать производительность труда при выполнении работ с использованием различного оборудования. Все эти данные позволят повысить уровень профессиональной подготовки специалистов, послужат базовым и справочным материалом для проведения последующих проверок и планирования других работ по защите информации.

### 3.2. Определение характеристик изъятых средств негласного съёма информации.

i

По традиции, берущей своё начало со времён МГБ-КГБ, сбор данных о средствах НСИ возложен на органы ФСБ. Поэтому найденные в ходе проверки помещений подслушивающие, подглядывающие и тому подобные устройства рекомендуются сдавать соответствующие государственные органы, тем более что сбыт или использование по прямому назначению подобных устройств преследуются по закону. Тем не менее, перед сдачей обнаруженных средств НСИ целесообразно их сфотографировать и хотя бы грубо определить их технические и эксплуатационные характеристики. Эта процедура преследует, как минимум, две цели: во-первых, пополнение профессиональных знаний специалистов по защите информации, во-вторых, подготовка ответов на вопросы, которые неминуемо возникнут у руководства предприятия при получении известий о находке средств НСИ.

Первая цель не нуждается в пояснении. В случае обнаружения нестандартного, не описанного в специальной литературе и ранее не встречавшегося в поисковой практике средства НСИ, необходимо возможно более полное исследование его характеристик, провести которое можно

тальковусловиях лаборатории, оснащённой соответствующей измерительной и исследовательской аппаратурой. При этом наибольший интерес представляют следующие характеристики и особенности неизвестного средства НСИ:

- применённые способы перехвата (съёма), преобразования (в том числе, закрытия) и передачи информации;
- особенности маскировки;
  - ориентировочное время жизни (длительность функционирования), ресурса работы от автономного источника питания;
  - технические характеристики средства НСИ, определяющие дальность его действия и требования к поисковой аппаратуре (вид и мощность сигнала, его рабочая частота, вид и ширина спектра, вид модуляции, наличие побочных излучений и т.д.);
- возможность накопления информации, изменения характеристик и режимов работы средства (например, встроенным активизатором включения), дистанционного управления его работой;
- технический и технологический уровень изделия, нестандартные решения, принятые при разработке, изготовлении и установке средства НСИ.

По результатам исследования для руководства предприятия подготавливается справка о потребительских характеристиках найденного нестандартного средства НСИ.

Если же в ходе проверки помещений был обнаружен уже знакомый, встречавшийся ранее тип средства НСИ, членам поисковой бригады следует подготовить справку по найденному экземпляру этого типа. Руководство предприятия обычно интересуется не технические характеристики изделия, а сведения, позволяющие оценить возможный ущерб, нанесённый средством НСИ. В первую очередь его будет интересовать:

- информацию какого вида и в какой зоне перехватывало найденное средство НСИ;
- работоспособность обнаруженного средства на момент проверки;
- давность установки средства НСИ;
- особенности работы обнаруженного устройства: постоянно или периодически осуществлялся съём информации, в реальном масштабе времени или с задержкой осуществлялась её передача, каким образом осуществлялась активизация средства НСИ.

Для предотвращения возможного повторного использования противником аналогичного средства руководство предприятия должно знать применённый противником способ установки (внедрения) средства НСИ, дальность передачи перехватываемой информации или используемый способ съёма противником накапливаемой информации.

Для получения ответов на эти вопросы обычно не требуется строгих инструментальных исследований. Существует достаточно много признаков, позволяющих путём внешнего осмотра места установки средства НСИ, самого устройства, а также путём анализа его сигналов с помощью поисковой аппаратуры оценить возможные значения характеристик устройства. Так, например, наличие подсоединённого к устройству микрофона или небольшого отверстия в корпусе устройства указывает на то, что оно осуществляло съём акустической информации. Ориентируясь на характеристики известных радиомикрофонов и сетевых микрофонов [15,16,19], можно с высокой степенью достоверности предположить, что радиус съёма акустической информации таким устройством в обычных условиях не превышает шести-восьми метров.

Подключение устройства к проводной линии говорит о возможном съёме устройством информации с линии и (или) возможном использовании линии в качестве источника питания. По типу или габаритам автономного источника питания можно судить о его ёмкости, а измерив ток потребления средства НСИ, можно рассчитать возможную продолжительность непрерывной работы устройства. По относительному уровню сигнала и значению его несущей частоты можно судить о возможной дальности его распространения. Давность установки средства НСИ в случае его питания от автономного источника можно оценить по сохранившемуся ресурсу (степени разряда) источника питания.

При невозможности провести прямые измерения характеристик найденного устройства можно попытаться провести его идентификацию с описанными в специальной литературе средствами НСИ [15,16,17,18,19, 20,21]. Основными идентификационными признаками при этом могут быть внешний вид и назначение устройства (вид снимаемой информации), его весогабаритные характеристики, параметры энергопотребления и другие установленные в процессе поиска характеристики устройства.

Результаты этих работ должны пополнить вашу картотеку или базу данных по средствам НСИ.

### 3.3. Составление описания проведённых работ.

Обычно в число отчётных документов включается *описание проведённых поисковых и исследовательских работ* с приложением поясняющих схем, рисунков, протоколов измерений, необходимых инженерно-технических выкладок. Если план проведения комплексной специальной проверки помещений был разработан достаточно подробно и тщательно, составление описания работ не вызывает трудностей. По

своему содержанию и объёму описание работ может быть развёрнутым и подробным или достаточно лаконичным. Объём, как и необходимость составления этого документа, целесообразно заранее согласовать с руководством предприятия.

Мы рекомендуем следующую структуру развёрнутого описания работ:

- вводная часть, содержащая целевую установку, время проведения проверки, перечень и краткую характеристику проверенных помещений, численный состав поисковой бригады, перечень использованных в ходе проверки приборов и оборудования;
- основная часть, включающая отдельно для каждого помещения:
  - перечень проведённых поисковых и исследовательских работ с указанием данных, отражающих трудозатраты на их проведение (площадь обследованных элементов ограждающих конструкций, количество и степень сложности проверенных предметов обстановки, длина проверенных коммуникаций и др.);
  - описание каждой работы с указанием заводских номеров и даты последних проверок аппаратуры, использованной для проведения измерений, методики проведения измерений;
    - результаты (протоколы) измерений и работы в целом (уровни сигналов, их частоты и другие параметры, обнаружено средство НСИ или нет, выявленные каналы возможной утечки защищаемой информации);
  - план помещения с указанием мест размещения аппаратуры, обнаруженных средств НСИ и технических каналов утечки защищаемой информации.

Уместно ещё раз напомнить, что современные программно-аппаратные комплексы обычно обеспечивают автоматическое формирование протоколов измерений и отчётов (приложение 7). Эти документы целесообразно включить в состав описания работ в качестве приложений.

### 3.4. Разработка рекомендаций по повышению защищённости помещений.

Для руководства предприятия, заказавшего проведение комплексной специальной проверки помещений, наибольший интерес, помимо результатов поиска средств НСИ, представляют *рекомендации по повышению защищённости проверенных помещений* и предотвращению съёма защищаемой информации по выявленным потенциальным техническим каналам её утечки. В зависимости от объёма и степени детализации, эти рекомендации могут составлять отдельный отчётный документ.



Такие рекомендации обычно включают:

- перечень выявленных потенциальных ТКУИ для каждого проверенного помещения;
- схемы выявленных потенциальных ТКУИ с краткими пояснениями (легендами);
- оценку вероятности использования противником потенциальных ТКУИ и существующей на время проверки защищённости каждого помещения от негласного съёма информации по выявленным потенциальным ТКУИ;
- конкретные рекомендации по мерам и способам предотвращения съёма защищаемой информации по выявленным ТКУИ и повышению защищённости помещений по каждому ТКУИ:
  - рекомендации по организационным, в том числе, режимным мерам;
  - рекомендации по изменению элементов конструкции помещений, инженерно-технических коммуникаций и другим инженерным мерам устранения потенциальных ТКУИ;
  - рекомендации по установке специальных приборов и систем защиты, в том числе, комплексных систем защиты помещений от утечки информации по техническим каналам, и другим техническим мерам повышения защищённости помещений;
  - сводный перечень технических средств и систем защиты информации, рекомендуемых к установке на предприятии для повышения защищённости помещений;
- предложения по практическому использованию рекомендуемых технических средств и систем и объединению их в единую комплексную систему защиты информации.

Как это следует из определения, потенциальные ТКУИ отличаются от реальных только своей временной неостребованностью, то есть временным отсутствием в своём составе средств разведки противника. Перечень выявленных потенциальных ТКУИ обычно состоит из естественных (непреднамеренных) каналов. В отличие от искусственно созданных, естественные ТКУИ не обеспечивают комфортных условий приёма перехваченной информации, но существуют постоянно и могут быть использованы противником в любой момент.

Выявление и строгая количественная оценка потенциальных ТКУИ требует специальных измерений и исследований, проводимых по особым методикам и, как правило, не включаемых в число работ по комплексной специальной проверке помещений. Вместе с тем, руководство предприятия обычно ожидает от поисковой бригады хотя бы качественной оценки степени защищённости помещений от утечки информации.

В этой связи целесообразно заранее, ещё на этапе подготовительных работ выяснить у руководства предприятия, нужны ли ему дорогостоящие

специальные исследования для получения точных количественных оценок защищённости помещений, или можно ограничиться качественными критериями. В подавляющем большинстве случаев достаточно знать, имеются ли в помещении незакрытые потенциальные технические каналы утечки информации, и может ли выявленный противник воспользоваться этими каналами для съёма информации. В остальных случаях приходится ограничиваться указанием зон энергетической доступности источников информативных сигналов, ранжированием выявленных каналов утечки информации по степени угроз, экспертными оценками вероятности съёма информации различными видами специальных технических средств и другими аналогичными показателями.

Приемлемая качественная оценка возможности утечки защищаемой информации через разнообразные (см. приложение 2) потенциальные ТКУИ может быть получена путём анализа сведений о конструктивных особенностях здания и помещений, визуального осмотра проверяемых и соседних с ними помещений и проверки наличия информативных сигналов на «концах» потенциальных ТКУИ, доступных противнику. Такую проверку наличия информативных сигналов целесообразно проводить на границе *контролируемой зоны*, под которой обычно понимается пространство или территория, в пределах которых исключено неконтролируемое пребывание посторонних лиц.

Стандартный набор специального оборудования и технических средств, рекомендованный нами для проведения комплексной специальной проверки помещений объектов (таблица 1), позволяет членам поисковой бригады «сработать за противника», имитируя его действия по съёму защищаемой информации с потенциальных ТКУИ. Так, оценить степень слышимости и разборчивости акустических и виброакустических сигналов на границе контролируемой зоны вокруг проверяемых помещений можно с помощью многофункционального поискового прибора ПИРАНЬЯ. Приборы поиска сигналов в проводных линиях позволяют оценить возможность съёма информации противником за счёт «микрофонного» эффекта и наводок. Комплекс обнаружения радиоизлучающих средств и радиомониторинга КРОНА-6000М даёт возможность сравнить уровни информативных ПЭМИ средств оргтехники с уровнями известных (эталонных) источников излучения.

Следует, тем не менее, хорошо понимать, что эти приборы позволяют симитировать средства разведки не слишком изощрённого, технически слабовооружённого противника, поскольку ориентированы, главным образом, на поиск преднамеренно созданных, «комфортных» ТКУИ. Поэтому для полномасштабных исследований ПЭМИ, звуко- и виброизоляции помещений, акустических и виброакустических сигналов и наводок следует применять специально разработанный аппаратный комплекс типа НАВИГАТОР, СПРУТ-5 или ил ии подобную измерительную аппаратуру.

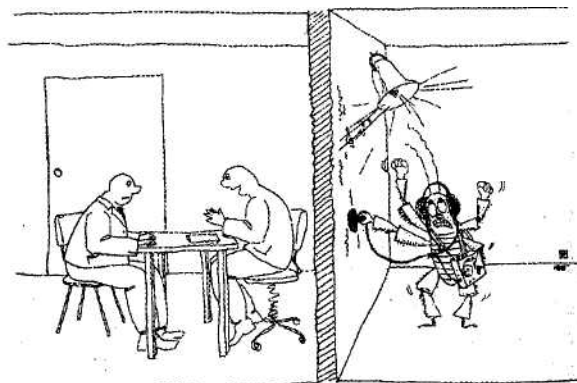
С учётом этих соображений, при отсутствии специальных исследований можно допустить грубую оценку вероятности использования противником потенциальных ТКУИ по субъективной слышимости или регистрации приборами информативных сигналов из проверяемого помещения на границе контролируемой зоны. При такой оценке вероятность использования противником потенциального ТКУИ можно считать *высокой*, если информативные сигналы слышны и разборчивы, уверенно регистрируются приборами.

В случае слабой разборчивости информативных сигналов использование противником потенциального ТКУИ приходится считать вполне возможным, поскольку для специалистов не составляет особого труда применить известные способы и средства шумочистки сигналов. Вероятность использования противником такого потенциального ТКУИ можно считать *средней*.

Наконец, если сигналы из проверяемого помещения регистрируются поисковой аппаратурой на фоне шумов, но их информативная значимость не ясна, то использование противником потенциального ТКУИ можно считать маловероятным, однако полностью исключить возможность использования противником таких сигналов всё же нельзя. Мы рекомендуем считать вероятность использования противником такого потенциального ТКУИ *малой*.

При отсутствии специальных исследований допустима чисто качественная оценка существующей на время проверки защищённости помещения от негласного съёма информации по техническим каналам её утечки. Учитывая множественность потенциальных ТКУИ, в оценке защищённости помещения справедлив известный подход к оценке прочности цепи, состоящей из множества звеньев: её прочность определяется наиболее слабым звеном. В нашем случае «слабость звена» может оцениваться вероятностью использования противником конкретного потенциального ТКУИ. Поэтому помещение можно считать *незащищённым* от негласного съёма информации в случае, если существует высокая вероятность использования противником хотя бы одного выявленного ТКУИ.

Рекомендации по мерам и способам предотвращения съёма информации по выявленным ТКУИ



следует давать отдельно для каждого помещения и каждого потенциального ТКУИ. В периодических изданиях и специальной литературе достаточно широко освещены возможные способы защиты информации от утечки по техническим каналам [3,4,15,17,18,20]. Их перечисление и оценка не входят в число поставленных при написании данной работы задач. Отметим только, что во многих случаях наиболее эффективным и дешёвым способом перекрытия технических каналов утечки информации может стать применение активных систем шумления (акустического, виброакустического, пространственного электромагнитного и линейного электрического). В качестве примеров таких систем можно назвать комплекс виброакустической защиты БАРОН, устройства активной защиты информации УАЗИ, генераторы шума ГРОМ-ЗИ и другие аналогичные приборы.

При выборе способов и средств для перекрытия выявленных ТКУИ необходимо в первую очередь 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». Обоснованные таким образом рекомендации всегда будут с благодарностью восприняты руководством предприятия.

Следует также помнить, что утечка информации может проходить не только по техническим каналам. Поэтому в рекомендациях по установке технических средств и систем не следует забывать о средствах скрытого наблюдения, регистрации действий посетителей и персонала, системах сигнализации, блокировки ит.п. Системы гласного, осуществляемого с ведома и согласия персонала видеоконтроля, акустического мониторинга помещений, регистрации телефонных переговоров во многих случаях оказываются более действенными для предотвращения утечки информации, чем физическая охрана контролируемой зоны или, к примеру, применение аппаратуры защиты от съёма информативных наводок.

За рекомендациями по способам и средствам предотвращения утечки информации по выявленным ТКУИ целесообразно разместить сводный перечень технических средств и систем защиты информации, рекомендуемых к установке на предприятии. Хорошо, если в перечне будет указан, помимо основного варианта, один или два аналога рекомендуемого средства защиты, тем более что сегодня на рынке предлагается достаточно большое количество примерно однотипных средств. Не следует забывать о включении в перечень средств и систем контроля за работоспособностью и эффективностью рекомендованной техники защиты информации. Перечень также должен отражать количество однотипных средств, требуемое для перекрытия всех опасных ТКУИ в проверенных помещениях.

Документ целесообразно завершить предложениями по практическому использованию средств и систем защиты информации, рекомендуемых к установке на предприятии, и объединению или внедрению рекомендуемых технических средств и систем в единую комплексную систему защиты информации на предприятии. В предложениях по практическому использованию средств и систем защиты можно указать, в каком временном режиме целесообразно использовать средства защиты (кратковременно, постоянно или периодически), кем должно приниматься решение на их применение, комплексно или по отдельности их лучше применять, как контролировать их работоспособность и эффективность, целесообразно ли вводить централизованное управление работой средств защиты и контроля и т.п.

Следует иметь в виду, что интеграция отдельных средств в систему защиты информации в единую комплексную систему, как правило, даёт заметный выигрыш в качестве защиты информации. Во время расхода на защиту информации если и увеличиваются, то незначительно. Повышение эффективности защиты информации происходит, главным образом, за счёт централизованного управления ресурсами системы, повышения качества контроля за работой составляющих её технических средств, возможности быстрого реагирования на возникновение новых угроз утечки информации.

Первой ступенью интеграции может быть создание условий для оперативного контроля занятости, работоспособности технических средств защиты информации и контроля, их быстрой замены или перенацеливания. Это может быть сделано, например, путём сведения этих средств в специально выделенное помещение и оборудования в нём поста контроля защиты информации. Современные средства и системы защиты информации, обеспечивающие возможность дистанционного управления их работой, контроля их эффективности, позволяющие одновременно контролировать фазу несколько помещений, существенно облегчают решение этой задачи.

Последующие ступени интеграции предусматривают обеспечение конструктивной, информационной, программной и эксплуатационной совместимости технических средств защиты информации и контроля. Одним из примеров интеграции различных средств и систем защиты помещения от утечки акустической информации может служить разработанный НПЦ Фирма «НЕЛ К» комплекс защиты речевой информации КЗРИ-1, базовый вариант которого включает систему защиты телефонных линий «Прокруст-2000», систему виброакустического шумления «Барон» и подавитель радиоэлектронных устройств негласной аудиозаписи «Шторм».

В приложении? приведён пример возможных рекомендаций руководству предприятия по повышению защищённости помещений, разработанных по результатам комплексной специальной проверки помещений в виде отдельного документа.

### 3.5. Составление акта проведения комплексной специальной проверки помещений.

Основным итоговым документом, завершающим работы по обследованию помещений на наличие средств НСИ, является *акт проведения проверки*. Этот документ обычно включает:

- время проведения обследования;
- состав поисковой бригады;
- перечень обследованных помещений и объектов;
- перечень и объём основных поисковых работ и сопутствующих исследований;
  - перечень использовавшейся поисковой и исследовательской аппаратуры;
  - результаты проверки:
    - где были обнаружены средства НСИ, их состояние и краткие характеристики;
    - принятые по отношению к обнаруженным средствам меры (изъятие, нейтрализация, консервация с целью последующей дезинформации);
    - выводы из оценки степени защищённости помещений и объектов от утечки защищаемой информации по различным каналам;
      - рекомендации по повышению защищённости помещений и объектов и предотвращению утечки информации по выявленным техническим каналам её утечки.

Акт обычно подписывается руководителями членами поисковой бригады, согласовывается с руководителем организации, проводившей поисковые работы, после чего предоставляется для утверждения руководителю предприятия (фирмы) или начальнику его службы безопасности.

В приложении 5 приведён формализованный вариант акта проведения комплексной специальной проверки помещений.

### 3.6. Завершающие работы заключительного этапа.

К завершающим работам заключительного этапа следует отнести оформление итоговых и отчётных документов, подготовку к заключительной встрече с руководством предприятия и, наконец, представление руководству предприятия разработанных по результатам проверки документов для утверждения.

Оформление документов по результатам проверки заключается в

изготовлении необходимого числа экземпляров текстуальных и графических документов, их строгом учёте в соответствии с принятой системой регистрации и учёта документов, содержащих конфиденциальную информацию, в подписании документов руководителем и членами поисковой бригады и согласовании содержания документов с руководством организации, проводившей проверку помещений. В случае проверки помещений силами сторонней организации в число документов, подготавливаемых для передачи руководству предприятия, включаются также учётные и регистрационные журналы.

Опыт проведения комплексных специальных проверок помещений свидетельствует о том, что представление подписанных и согласованных документов для утверждения руководству предприятия, заказавшему проведение проверки, обычно выливается в беседу по вопросам защиты информации. В этой связи специалистам рекомендуется тщательно подготовиться к заключительной встрече с руководством предприятия, чтобы убедительно доказать обоснованность и необходимость выполнения рекомендаций по повышению защищённости помещений от утечки информации. Следует быть готовым к ответам на вопросы не только по поводу эффективности того или иного рекомендованного способа или средства защиты, но и к обоснованию затрат, необходимых для реализации каждой рекомендации. Поэтому целесообразно заранее подготовить каталоги современных технических средств и систем защиты информации, необходимые справки и выкладки, прайс-листы фирм и организаций, занимающих в этой области ведущие позиции. Хорошо, если перед встречей

с руководством  
предприятия  
специалистам  
организации,  
проводившей  
проверку,  
удастся  
обсудить с  
начальником  
службы  
безопасности  
предприятия  
содержание  
рекомендаций  
и убедить  
его в их  
целесообразности.



В ходе встречи с руководством предприятия для утверждения итоговых и отчётных документов рекомендуется раскрыть структуру документов, устно пояснить содержание отдельных пунктов, всесторонне обосновать содержащиеся рекомендации, поднять вопрос о сроках проведения следующей проверки помещений. Целесообразно подчеркнуть, что успешное проведение «зачистки» помещений не должно успокаивать руководство предприятия, поскольку очередная атака на его секреты может начаться в любое время.

Пользуясь удобной возможностью довести до руководителя современные взгляды на систему информационной безопасности предприятия, можно в тактичной форме указать на необходимость ведения постоянного, а не периодического радиомониторинга важных служебных помещений. Это обусловлено всё возрастающим распространением дистанционно включаемых радиоизлучающих средств НСИ, а также высокой вероятностью и простотой подброса радиомикрофонов в любое удобное для противника время. Радиомикрофон, например, может быть скрытно занесён и включён во время переговоров кем-то из его участников. Следует также указать, что только ведение круглосуточного непрерывного радиомониторинга позволяет надёжно выявить радиоизлучающие средства НСИ с промежуточным накоплением информации и использующие для передачи информации в сжатом виде режим быстрогодействия.

Весьма высока вероятность внедрения противником средств НСИ в ПЭВМ или другие электронные приборы, особенно во время их ремонта или профилактического осмотра. Во время выявления таких средств довольно сложная задача. В этой связи можно напомнить, что в важных служебных помещениях рекомендуется размещать только сертифицированные технические средства, прошедшие предварительный визуальный осмотр и специальную проверку. Целесообразно подчеркнуть, что такую процедуру должны проходить не только новые электронные приборы, но и любые новые предметы и подарки, включая книги, видеокассеты, зажигалки и т.п.

В заключение встречи можно указать, что средства и методы негласного съёма информации постоянно совершенствуются, поэтому организационные и технические решения, сегодня эффективно препятствующие утечке конфиденциальной информации, могут в скором времени оказаться недостаточными. В этой связи созданная на предприятии служба безопасности и техническая система информационной безопасности должны развиваться с темпами, по крайней мере, не отстающими от нарастания угроз.

Следует помнить, что принятие решения по разработанным рекомендациям и всем обсуждавшимся вопросам остаётся за руководителем предприятия, поэтому изложение рекомендаций должно вестись в убедительной, но ненавязчивой и тактичной форме. Если в ходе этой встречи удастся достичь взаимопонимания, можно быть уверенным, что результаты специальной проверки выразятся не только в «чистоте» проверенных помещений, но и в общем повышении уровня защиты информации на предприятии.



---

## Заключение

Этой публикацией мы хотели привлечь внимание специалистов, прежде всего, к организационным и методическим вопросам проведения комплексных специальных проверок помещений. Изложенные в данной работе рекомендации безусловно не исчерпывают всего многообразия задач и проблем, возникающих в процессе поиска средств негласного съёма информации. Многие из них остались за рамками публикации. Не вошло в брошюру и изложение современных методик выявления потенциальных технических каналов утечки информации.

Представленные в брошюре методические рекомендации соответствуют современному уровню развития средств перехвата информации и её защиты. Однако, как те, так и другие средства развиваются непрерывно. Совершенствуются и методы, применяемые противником для добывания информации. В этой связи методика поиска средств негласного съёма информации не может и не должна представлять собой застывшую догму. Появление новых, более совершенных образцов досмотровой, поисковой и исследовательской техники неизбежно вызовет необходимость корректировки изложенных здесь рекомендаций. Поэтому данные материалы должны рассматриваться специалистами лишь в качестве ориентира в своей работе по поиску и нейтрализации различных источников информации в различных устройствах. Любые предложения специалистов по совершенствованию данной методики будут с благодарностью восприняты авторами публикации.

В заключение ещё раз подчеркнём, что проведение комплексных специальных проверок помещений не может защитить охраняемые сведения от всех видов угроз. Только постоянно развивающаяся *система информационной безопасности* может сдерживать натиск непрерывно совершенствующихся средств и методов негласного съёма информации. Убедить руководство предприятий и фирм в необходимости создания такой системы - одна из насущных задач руководителей служб безопасности этих организаций.

Непрерывно возрастающему уровню угроз должен быть противопоставлен постоянный рост технической оснащённости, профессиональных знаний, умений и навыков специалистов, работающих об охране информации.

## Приложение 1.

### Словарь основных терминов и определений

**Закладочное устройство** - элемент средства (системы) негласного съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

**Защищаемая информация** - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

**Информативное побочное электромагнитное излучение (ПЭМИ)** - побочное электромагнитное излучение, содержащее информацию о сведениях, относимых к защищаемой информации.

**Информативные наводки** - наводки, содержащие информацию о сведениях, относимых к защищаемой информации.

**Информативный (опасный) сигнал** - сигнал (звуковой, зрительный, электромагнитный и др.), содержащий информацию о сведениях, относимых к защищаемой информации.

**Информация** - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

**Канал утечки информации** - физический путь, по которому происходит утечка защищаемой информации от её источника к противнику.

**Контролируемая зона** - пространство или территория, в пределах которых исключено неконтролируемое пребывание посторонних лиц.

**Легенда прикрытия** - вымышленные сведения о намечаемых или проводимых действиях, мероприятиях, скрывающие их подлинный характер и истинное предназначение.

**Наводки** - токи и напряжения в токопроводящих элементах, вызванные электромагнитным излучением, емкостными и индуктивными связями.

**Несанкционированный доступ к информации** - получение защищаемой информации заинтересованным физическим лицом, группой лиц, организацией с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации.

**Обработка информации** - совокупность операций сбора, накопления, ввода, вывода, приема, передачи, записи, хранения, регистрации, уничтожения, преобразования, отображения информации.

---

**Объект специальной проверки** - помещения, объекты, предназначенные для ведения конфиденциальных переговоров, здания, сооружения, технические средства, в которых установлены средства (системы) обработки информации средства обеспечения объекта.

**Паразитное электромагнитное излучение** - побочное электромагнитное излучение, вызванное паразитной генерацией в электрических цепях технических средств обработки информации.

**Побочное электромагнитное излучение (ПЭМИ)** - нежелательное электромагнитное излучение, возникающее при работе технических средств.

**Проверяемое помещение** - помещение, в котором проводятся работы по поиску средств негласного съёма информации или оценке возможных технических каналов её утечки. Рассматривается в виде совокупности ограждающих помещение строительных конструкций, элементов находящихся в нём проводных, инженерно-технических и других коммуникаций, размещённого в нём оборудования, технических средств и систем обработки информации, мебели, других внесённых предметов и материалов.

**Противник** - организация, группа физических лиц или отдельное физическое лицо, предпринимающее неправомерные попытки получить доступ к чужой защищаемой информации, приводящий к нанесению ущерба её собственнику, владельцу или пользователю.

**Радиомониторинг** - деятельность по изучению и контролю радиоэлектронной обстановки, поиску и обнаружению источников радиоизлучений в районе объекта специальной проверки.

**Средство (система) негласного съёма информации (средство НСИ)** - специальное техническое средство (система) или совокупность технических средств, применяемых противником для преобразования, передачи, приёма (перехвата) и регистрации информативных сигналов с целью получения неправомерного доступа к чужой защищаемой информации.

**Технический канал утечки информации (ТКУИ)** — совокупность источника информативного (опасного) сигнала, физической среды, в которой распространяется этот сигнал, и технических средств противника, применяемых им для преобразования, передачи, приёма (перехвата) и регистрации этого сигнала.

**Утечка информации** - неконтролируемое распространение защищаемой информации за пределы организации или круга лиц, которым она доверена, в результате её разглашения, несанкционированного доступа к информации или получения защищаемой информации разведками.

---

Приложение 2.

Классификация технических каналов утечки информации  
(вариант).

1. *Общая классификация технических каналов утечки информации:*

---

Технические каналы утечки **информации**

---

по происхождению	по степени функционирования	по физической природе образования
искусственные (преднамеренно созданные)	реальные (действующие.) (включающие средство НСИпротивника)	акушческие (в том числе, акусижо- дреобразовательные)
естественные	потенциальные (не используемые противником)	электромагнитные (в том числе, магнитные и электрические)

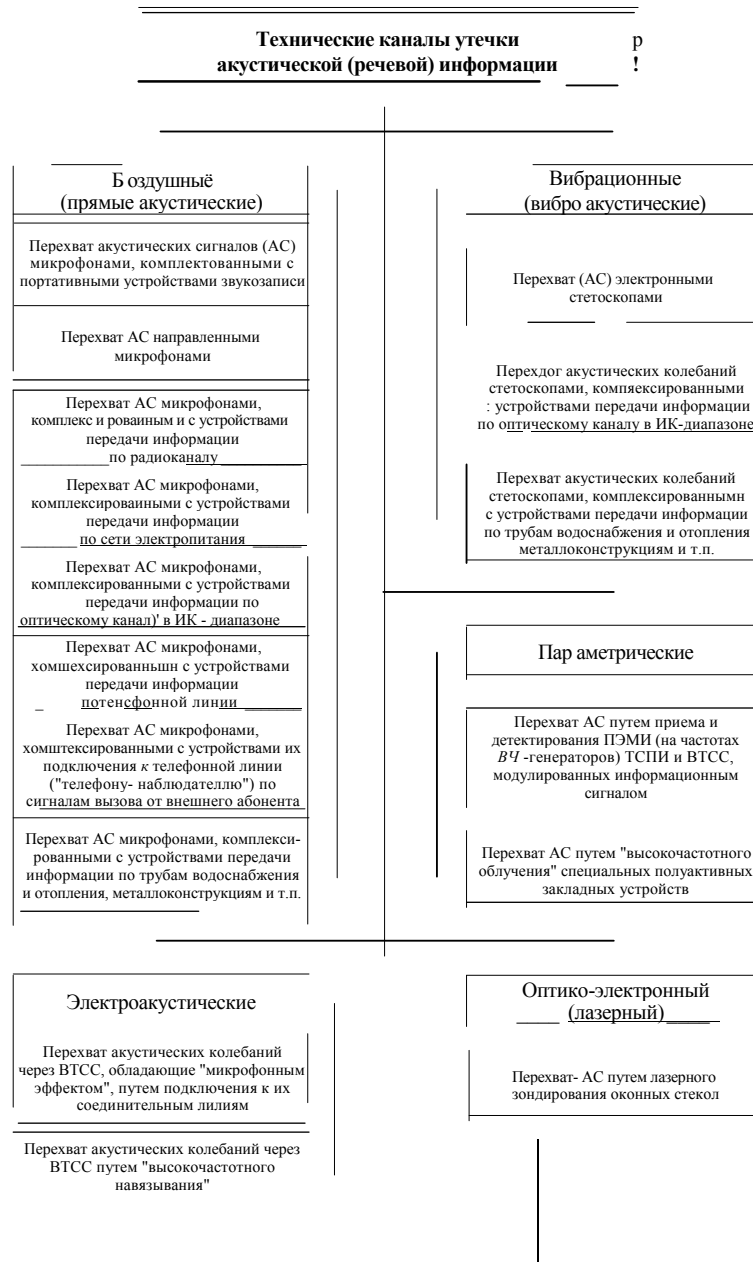
---

визуально - оптические

2. Классификация технических каналов утечки информации, обрабатываемой в технических средствах приёма, обработки, хранения и передачи информации (ТСПИ) [22]:

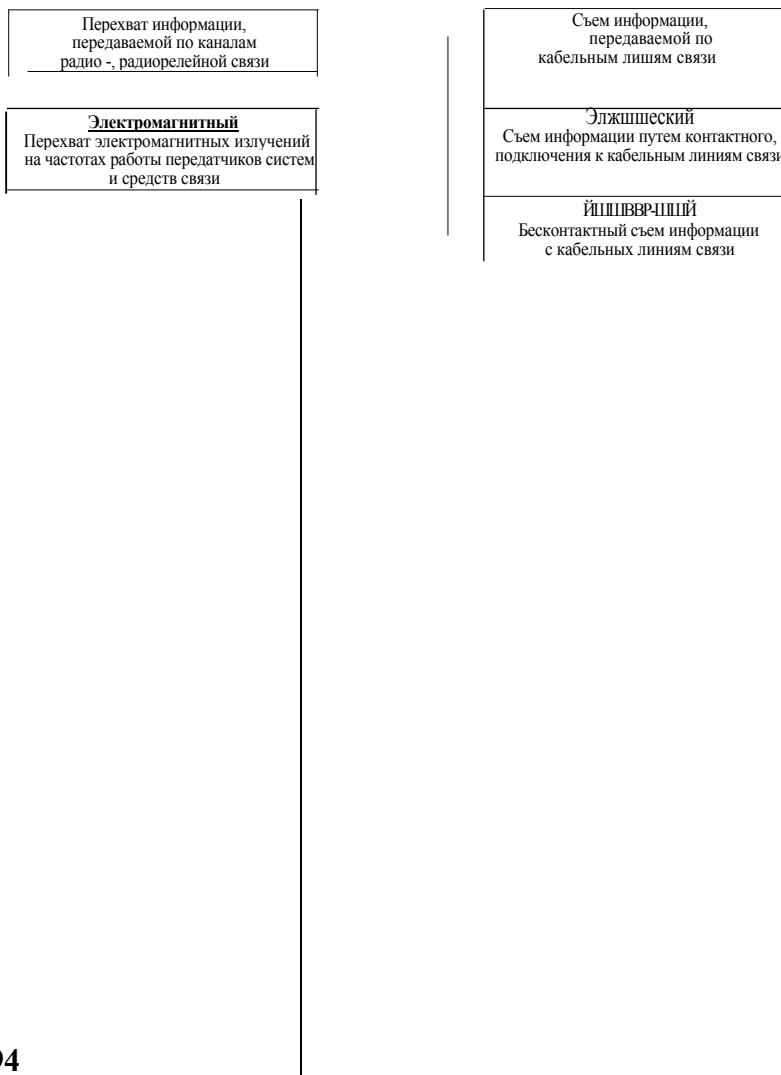


3. Классификация технических каналов утечки акустической (речевой) информации [22]:



4. Классификация технических каналов перехвата информации, передаваемой по каналам связи [22]:

Технические каналы перехвата информации,  
передаваемой по каналам связи



### Приложение 3.

Перечень специального оборудования и технических средств, рекомендуемых для проведения комплексной специальной проверки помещений.

*Таблица 2*

№ n/n	Наименование оборудования и технических средств	Виды работ, при которых используются оборудование и технические средства
1	Комплект досмотровых зеркал ( <b>ПОИСК-2, ШМЕЛЬ-2</b> )	Визуальный осмотр оборудования, мебели, технологических коммуникаций
2,3	Комплект луп, фонарей	Визуальный осмотр поверхностей и отверстий
	Технический эндоскоп с дистальным концом (серия <b>ЭТ, Olympus</b> )	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 ( <b>УНИСКАН 7215, АКА 7202, Comet</b> )	Проверка предметов и элементов интерьера на наличие металлических включений
6	Прибор нелинейной радиолокации ( <b>NR-900EM, ОРИОН NGE-400, РОДНИК 23</b> )	Проверка строительных конструкций и предметов на наличие радиоэлектронных компонентов
7	Переносная рентгеновизионная установка ( <b>ШМЕЛЬ 90/К, ФП-1, РОНА</b> )	Проверка элементов интерьера на наличие скрытно установленных средств НСИ
8	Переносный радиоприёмник или магнитола	Озвучивание проверяемых помещений
9	К&#x043e;функциональный прибор ( <b>ШИРАНЯ, ПСЧ-5, D-008</b> )	Проверка проводных коммуникаций на наличие информационных сигналов
10	Низкочастотный нелинейный детектор проводных коммуникаций ( <b>ВИЗИР</b> , возможная замена по телефонным линиям: <b>ТПУ-4f</b> или <b>SEL SP-18/T</b> )	Проверка проводных коммуникаций на наличие нелинейности параметров линии
11	Комплекс обнаружения радиоизлучающих средств и радиомониторинга ( <b>КРОНА-6000M, КРК, АРК-Д1, OSC-5000</b> )	Анализ радиоэлектронной обстановки, выявление радиоизлучающих средств негласного съёма информации
12	Обнаружитель скрытых видеокамер ( <b>IRIS VCF-2000</b> , нет аналогов)	Выявление радиоизлучающих видеокамер
13	Дозиметр поисковый ( <b>PM-1401, НПО-3</b> )	Обнаружение и локализация источников радиоактивного излучения
14	Комплекс для проведения исследований на сверхнормативные побочные электромагнитные излучения ( <b>НАВИГАТОР, ЛЕГЕНДА, ЗАРНИЦА</b> )	Выявление информативных побочных электромагнитных излучений
15	Комплекс для проведения акустических и виброакустических измерений ( <b>СПРУТ-4А</b> )	Выявление акустических и виброакустических сигналов и наводок, исследование звуко- и виброизоляции, проверка систем шумления



**Приложение 4.****Справочные данные по распределению радиочастот.**

1. Обозначение диапазонов радиочастот в соответствии с Регламентом радиосвязи [24].

*Таблица 3*

<b>Условное обозначение</b>	<b>Диапазон частот</b>	<b>Метрическое обозначение</b>
<b>ОНЧ (VLF)</b>	3...30 кГц	<b>Мириаметровые волны</b>
<b>НЧ (LF)</b>	30...300 кГц	<b>Километровые волны</b>
<b>СЧ (MF)</b>	300...3000 кГц	<b>Гектометровые волны</b>
<b>ВЧ (HF)</b>	3...30 МГц	<b>Декаметровые волны</b>
<b>ОВ4 (VHF)</b>	30... 300 МГц	<b>Метровые волны</b>
<b>УВЧ, УКВ (UHF)</b>	300...3000 МГц	<b>Дециметровые волны</b>
<b>СВЧ (SHF)</b>	3...30 ГГц	<b>Сантиметровые волны</b>
<b>КВЧ (EHF)</b>	30...300 ГГц	<b>Миллиметровые волны</b>
<b>ГВЧ</b>	300...3000 ГГц	<b>Децимиллиметровые волны</b>



## 3. Распределение частот в диапазонах ОБЧ и УВЧ для Москвы [12].

Таблица 5

Частота, МГц	Распределение по службам
32,000...45,000	Радиотелефоны МВД, ГВФ, МПС, Мосэнерго, Мосстрой, такси, СКИ
32,025	Радиовывоз
40,650	Радиовывоз
42,000	Промышленные ВЧ-установки
46,610...46,900	Беспроводной телефон (базовая станция)
49,000	Беспроводной телефон (трубка)
49,750/56,250	1-й канал ТВ, несущие изображения и звука
59,250/65,750	2-й канал ТВ, несущие изображения и звука
60,000...65,000	Радиотелефоны ГВФ, СКЭ, радиорелейные линии (РРЛ)
66,450...73,820	Радиовещание
75,000	ГВФ (связь с самолетами)
77,000...78,000	РРЛ
77,250/83,750	3-й канал ТВ, несущие изображения и звука
81,360	Промышленные ВЧ-установки
85,250/91,750	4-й канал ТВ, несущие изображения и звука
86,000...87,000	РРЛ
93,250/99,750	5-й канал ТВ, несущие изображения и звука
100,000	ГВФ
100,500...106,800	Радиовещание
108,100...112,000	ГВФ
118,000...136,000	ГВФ, СКЭ (передача информации с ИСЗ)
144,100...144,850	Радиолюбители
145,083...145,850	Радиолюбители
148,000...149,000	МВД
150,025...150,900	Радиотелефон «Алтай»
151,000...154,750	МПС
151,150	Радиовывоз «Мультитон»
152,500	Промышленные ВЧ-установки
154,900	Мосгазопровод
156,500...158,870	МПС, Минздрав
160,075	Радиосвязь, спецсвязь
162,250...162,600	Техпомощь, Мосэнерго

Частота, МГц	Распределение по службам
162,750	Радиовывоз
163,425...166,000	Спецсвязь, радиовывоз
167,000...167,800	РРЛ - %!
167,450	Центральный радиоклуб :■■ iЩ V
167,550... 168,075	Мосэнерго •, 4* si I
168,100...168,325	Автодорожная служба
169,500...174,000	Спецсвязь
174,050...174,500	Радиотелефон «Алтай-1»
174,550... 174,900	Радиотелефон «Алтай-1»
175,250/181,750	6-й канал ТВ, несущие изображения и звука *
175,000...180,000	СКЭ (передача информации с ИСЗ), РРЛ
183,250/189,750	7-й канал ТВ, несущие изображения и звука
183,000...184,000	СКИ
186,000...189,000	РРЛ, СКЭ (передача информации с ИСЗ)
191,250/197,750	8-й канал ТВ, несущие изображения и звука
194,000... 196,000	РРЛ
199,250/205,750	9-й канал ТВ, несущие изображения и звука
200,000...205,000	СКЭ (передача информации с ИСЗ)
207,250/213,750	10-й канал ТВ, несущие изображения и звука
205,950...208,575	МВД
210,500...211,300	СКЭ (передача информации с ИСЗ)
215,250/221,750	11-й канал ТВ, несущие изображения и звука
218,500... 220,200	СКЭ (передача информации с ИСЗ)
223,250/229,750	12-й канал ТВ, несущие изображения и звука , а/
228,600...297,200	РРЛ *Щ
240,000...317,000	Каналы спутниковой связи
300,537...300,767	Радиотелефон (абоненты)
301,137...302,612	Радиотелефон «Алтай-3» (абоненты)
302,637...304,112	Радиотелефон «Алтай-3» (абоненты)
304,137...305,812	Радиотелефон «Алтай-3» (абоненты)
305,437...315,813	Радиотелефон
329,600...335,000	ГВФ (связь с самолетом)

Частота, МГц	Распределение по службам
336,537...336,763	Радиотелефон
337,137...338,612	Радиотелефон «Алтай-3» (центр)
338,637...340,112	Радиотелефон «Алтай-3» (центр)
340,137...340,813	Радиотелефон «Алтай-3» (центр)
341,438...341,813	Радиотелефон (центр) ■' "Ч&'■•
400,100...401,000	Метеоспутники
432,000	Радиолюбители
453,025...457,475	Сотовый телефон NMT-450 (абоненты)
460,000	Промышленные ВЧ-установки
463,025...467,475	Сотовый телефон NWT-450 (центр) *'
471,250/477,760	21-й канал ТВ, несущие изображения и звука !
479,250/485,750	22-й канал ТВ, несущие изображения и звука ' С. "
487,250/493,750	23-й канал ТВ, несущие изображения и звука ■ ■■'
495,250...790,750	(24-60)-е каналы ТВ с шагом 8 МГц
824,050...827,950	Сотовый радиотелефон AMP3 (абоненты)
831,050...833,950	Сотовый радиотелефон AMP3 (абоненты)
835,900...838,700	Сотовый радиотелефон AMP3 (абоненты) **
869,050...872,950	Сотовый радиотелефон AMP3 (центр)
876,050...878,950	Сотовый радиотелефон AMP3 (центр)
880,900...883,700	Сотовый радиотелефон AMP3 (центр)
890,900...893,700	Сотовый радиотелефон СЗМ (абоненты)
935,900...938,700	Сотовый радиотелефон СЗМ (центр)
1240,00...1300,00	Радиолюбители

*Основные технические характеристики сотовых систем радиотелефонной связи [13].*

Таблица 6

Характеристики системы связи	AMPS	NMT-450	GSM
Полосы частот на передачу, МГц:			
базовая станция	870.7.890	463...467.5	935...960
подвижная станция	825...845	453...457.5	890.1.915
Разнос дуплексных каналов, МГц	45	10	45
Разнос частот соседних каналов, кГц	30	25/20	200
Максимальный радиус соты, км	20	40	35
Общее число каналов	666	180/255	124

5. *Диапазоны частот других систем подвижной (мобильной) радиосвязи [17].*

Диапазон частот пейджинговых систем персонального радиовызова—  
80...930МГц

Диапазоны частот систем беспроводных телефонов:

■ аналоговых:

■ 46,610...46,930 МГц (базовая станция)/49,670...49,990 МГц  
(радиотелефонный аппарат) (в сети 10 каналов);

• 959,0125...959,9875МГц/914,0125...914,9875МГц(40каналов);

• 885,0125...886,9875МГц/930,0125...931,9875МГц(80каналов);

• 26,3125...26,4875МГц/41,3125...41,4875 МГц (10 каналов);

■ цифровых:

■ 804...868 МГц («Telepoint» —40 каналов);

• 866...962 МГц (32 канала);

• 1880...1990МГц(«БЕСТ»— 120 каналов).

Диапазоны частот ведомственных радиосетей с закреплёнными за абонентами каналами: 100.. 200,340.. 375,400.. 520 МГц.

Диапазоны частот радиосетей подвижной радиосвязи общего пользования(транкинговых, сотовых):

• 130... 174,403.. 512МГц (Smag Trunk-II, StarSite и др.) -разнос частот соседних каналов 12,5; 20 или 25 кГц;

• 380.. 400 МГц (TETRA) - разнос частот соседних каналов 25 кГц, дуплексный разнос радиоканалов для передачи и приёма -10 МГц;

• 806.. 825/851.. 869,896.. 901/935.. 940 МГц (Multi-Net и др.)-разнос частот приёма/передачи 45 МГц.

## Приложение 5.

### Формализованный вариант плана проведения комплексной специальной проверки помещений.

Конфиденциально

Экз. № \_

Всего \_ экз.

Согласовано  
Начальник службы безопасности предприятия

\_\_\_\_\_ /  
200 г.

Утверждаю  
Руководитель предприятия

\_\_\_\_\_ / \_\_\_\_\_ /  
" " 200 г.

#### План проведения комплексной специальной проверки помещений

##### 1. Выводы из оценки противника.

В качестве субъекта, выбранного вероятным противником для внедрения средств НСИ, рассматривается посетитель (клиент), имевший доступ в кабинет руководителя предприятия и в соседние с ним помещения. Для внедрения средств НСИ возможно использование противником одного из строительных рабочих, проводивших косметический ремонт кабинета руководителя в период с \_ по \_ (дата, время). В качестве субъекта, осуществляющего съём информации, рассматривается посетитель (клиент) или посторонние лица за пределами контролируемой зоны.

Субъект, осуществлявший внедрение средств НСИ, является специалистом по негласному съёму информации, обладает сведениями о расположении интересующих его помещений, размещении в них оборудования и предметов интерьера.

Учитывая возможность установки средств НСИ во время ремонта кабинета руководителя, можно ожидать использования противником как радиоизлучающих средств НСИ, так и передающих информацию по проводам. В соседних помещениях возможна установка противником средств съёма информации с телефонных линий и электронных стетоскопов. Ожидаемый

технический и технологический уровень применяемых средств НСИ соответствует среднему участку ценового диапазона этих средств.

Наиболее вероятно установка средств НСИ во время ремонта кабинета руководителя путём подброса, подключения к телефонной линии, подмены электроустановочных и телефонных коммутационных изделий. Возможен подброс радиомикрофона во время посещения кабинета посетителем (клиентом). Вероятное время установки (внедрения) средств НСИ - в период с \_\_ по \_\_ (дата, время). Ожидаемые способы съёма информации - подключение к проводным линиям в соседних помещениях и перехват радиопередач с помощью радиоконтрольного пункта, размещённого за пределами охраняемой территории.

При обнаружении противником намерений провести специальную проверку помещений возможно временное изъятие средств НСИ. Установление факта проведения такой проверки может привести к временному отключению дистанционно управляемых средств НСИ. При установлении факта обнаружения внедрённых средств НСИ наиболее вероятно попытка внедрения нового аналогичного устройства.

## **2. Замысел проведения комплексной специальной проверки помещений.**

***Цель проведения проверки - предотвращение ущерба от утечки информации из помещения через возможно внедрённые средства НСИ.***

*Проверке подлежат:*

1. Кабинет руководителя предприятия.

Площадь помещения - \_\_ кв. м., объём - \_\_ куб. м. Ограждающие конструкции - железобетонные панели (толщина наружной стеновой панели - \_\_ см, двух внутренних стеновых панелей - \_\_ см, пола и потолочного перекрытия - \_\_ см), смежная с бухгалтерией стена - кирпичная, толщиной - \_\_ см. Потолок подвесной, стены оштукатуренные, отделанные деревянными панелями. Два вентиляционных канала естественной вентиляции.

Телевизор, ПЭВМ, телефонный аппарат. Мебель стандартная офисная: письменный и журнальный столы, два стула, встроенный шкаф, два стеллажа, три мягких кресла, сейф, холодильник занимают \_\_ процентов общей площади помещения.

Проводные коммуникации силовой и осветительной сети, телефонная линия, линии пожарной и охранной сигнализации. Магистраль парового отопления.

2 Помещение бухгалтерии.

(приводятся характеристики второго помещения)



**Перечень запланированных работ:**

1. В кабинете руководителя предприятия:
  1. Визуальный осмотр ограждающих конструкций, мебели и других предметов интерьера (ожидаемая трудоёмкость - \_\_\_ чел. часов).
  - 2 Проверка элементов строительных конструкций, мебели и других предметов интерьера с использованием специальных поисковых технических средств ( \_\_\_ чел. часов).
  3. Проверка линий и оборудования силовой и осветительной электросети ( \_\_\_ чел. часов).
  4. Проверка линий и оборудования абонентской телефонной сети ( \_\_\_ чел. часов).
  5. Проверка линий и оборудования пожарной и охранной сигнализации ( \_\_\_ чел. часов).
  - & Проверка радиозфира на присутствие сигналов радиоизлучающих средств негласного съёма информации (радиомониторинг помещения) ( \_\_\_ чел. часов).
  7. Проверка несанкционированных передатчиков информации в диапазоне инфракрасного излучения ( \_\_\_ чел. часов).
  8. Поиск средств негласного съёма и передачи информации, внедрённых в электронные приборы ( \_\_\_ чел. часов).
- 2 На внешней, выходящей на улицу поверхности стены кабинета руководителя:
  1. Визуальный осмотр ограждающих конструкций ( \_\_\_ чел. часов).
  3. В помещении секретаря (смежном с кабинетом руководителя):

*(приводится перечень запланированных работ)*

4. В помещении бухгалтерии:

(далее продолжается перечень помещений и перечень запланированных в них работ)

**Время проведения специальной проверки:**

с (дата, время) до (дата, время) . Общая продолжительность непосредственного проведения проверки - \_\_\_ часов.

**Легенда прикрытия предварительного осмотра помещений:**

Осмотр помещений для составления сметы на монтаж системы принудительной вентиляции (с (дата, время) до (дата, время)). Доводится под запись до секретаря и ответственного за эксплуатацию здания за три дня до осмотра (дата).

Документ подтверждающий легенду - копия договора на выполнение

монтажных работ.

*Легенды прикрытия поисковых работ:*

1. Проверка специалистами телефонного узла связи состояния телефонных линий и оборудования (с (дата, время) до (дата, время)). Доводится под запись до секретаря за два дня до проверки ( дата ).

Документы, подтверждающие легенду - наряд на проведение работ и допуск для работ на оборудовании.

2 Поиск местонахождения искрящих контактов скрытой электропроводки для устранения помех ПЭВМ (с (дата, время) до (дата, время) ). Доводится до секретаря и ответственного за электрохозяйство накануне проверки (дата).

Документ подтверждающий легенду - копия договора на выполнение поисковых работ.

*Меры по активации внедренных средств съёма информации:*

Доведение до секретаря и лиц руководящего состава предприятия информации о проведении в день проверки совещания руководящего состава предприятия по вопросам ускорения разработки новых образцов продукции и продвижения их на рынок товаров и услуг. Способ доведения - распространение среди лиц руководящего состава повестки дня совещания и распоряжения о подготовки докладов. Дата доведения: \_\_\_\_ (за неделю до начала проверки).

*Действия в случае обнаружения средств негласного съёма информации:*

Не трогая обнаруженное средство, доложить о факте обнаружения руководителю и начальнику службы безопасности предприятия для принятия решения о дальнейших действиях.

i

**3. Привлекаемые силы и средства, их распределение по объектам и видам работ.**

*Состав поисковой бригады:*

1. - руководитель;
2. 3.

Перечень специального оборудования и технических средств, привлекаемых для проведения проверки:

1. Комплект досмотровых зеркал ШМЕЛ Ъ-2 (применяется только при закрытых дверях помещения и отсутствии в нём посторонних лиц).

2. Прибор нелинейной радиолокации NR-900EM (в процессе радиомониторинга не включать, применять только при закрытых дверях помещения и отсутствии в нём посторонних лиц).

3.

(далее продолжается перечень оборудования и технических средств с указанием основных особенностей их применения в рамках выбранных легенд прикрытия и других ограничений, налагаемых условиями проверки)

**Распределение специалистов поисковой бригады, оборудования и технических средств по видам работ и объектам специальной проверки:**

Специалист-исполнитель			Помещение	Время проведения	Виды работ	Технические средства
1	2	3				
+	+		Кабинет руководит.	с __ до __	Визуальный осмотр	ШМЕЛЬ-2, ЭТ-4-0,5АП, лупы, фонари
+				с __ до __	Проверка конструкций, мебели и предметов с использованием СПТС	NR-900EM, ФП-1, УНИСКАН 7215
		+		с __ до __	Проверка линий электросети	ПИРАНЬЯ, ВИЗИР
		+		с __ до __	Проверка линий телефонной сети	ПИРАНЬЯ, ВИЗИР
		+		с __ до __	Проверка линий сигнализации	ПИРАНЬЯ, ВИЗИР
+				с __ до __	Проверка радиоэфира	КРОНА-6000М, ПИРАНЬЯ
+				с __ до __	Проверка передач в ИК диапазоне	ПИРАНЬЯ
		+		с до	Поиск средств НСИ, внедрённых в электронные приборы	ПИРАНЬЯ, лупы
+			Бухгалтерия	с __ до __	Визуальный осмотр	ШМЕЛЬ-2, ЭТ-4-0,5АП, лупы, фонари
+				с __ до __	Проверка конструкций, мебели и предметов с использованием СПТС	NR-900EM, ФП-1, УНИСКАН 7215
<i>(далее таблица продолжается для всех проверяемых помещений и запланированных работ)</i>						

**Дополнительные меры по активизации внедренных средств НСИ:**

В кабинете руководителя для активизации средств НСИ с акустопуском с помощью магнитолы воспроизводятся предварительно сделанные на научной конференции записидокладов. В помещении бухгалтерии воспроизводятся предварительно сделанные записи обсуждения неконфиденциальных деловых вопросов. Начало воспроизведения записей - с началом проведения визуального осмотра ограждающих конструкций, мебели и др)тих предметов интерьера помещений.

При проверке наличия сигналов в проводных линиях всё подключённое к ним оборудование приводится в рабочее состояние (включается в рабочий режим), трубки телефонных аппаратов снимаются для перевода телефонных линий в режим «занято».

**4. Перечень подготавливаемых по результатам проверки итоговых и отчётных документов и срок их представления для утверждения.**

1. Акт проведения комплексной специальной проверки помещений. 2
- Описание проведённых работ и исследований.
3. Рекомендации по повышению надёжности защиты информации от её возможной утечки по техническим каналам.
4. Журнал регистрации заводских и инвентарных номеров оборудования, мебели и предметов.
5. Журнал регистрации пломб и скрытых меток. Ш

Акт проведения проверки помещений - в двух экземплярах (один - исполнителям работ). Остальные документы в единственном экземпляре.

Все документы - с грифом «конфиденциально». Срок представления для утверждения - \_\_\_\_\_.

*Согласовано*

Руководитель организации,  
проводящей проверку

\_\_\_\_\_/

" " 200 г.

Руководитель поисковой бригады

\_\_\_\_\_/ **И**  
**Члены поисковой бригады**

\_\_\_\_\_

200 г.

**Приложение 6.**

**Формализованный вариант акта проведения комплексной специальной проверки помещений.**

й

Конфиденциально  
Экз. № \_  
Всего экз. Ч

*Согласовано*  
Руководитель организации,  
проводившей проверку  
\_\_\_\_\_  
" " \_\_\_\_\_ 200 г.

*Утверждаю*  
Руководитель предприятия  
\_\_\_\_\_  
200 г.

**Акт проведения комплексной специальной проверки помещений**

1. В период с \_\_\_ по \_\_\_ на предприятии (наименование предприятия) проведена комплексная специальная проверка помещений. 2

Состав поисковой бригады:

1. \_\_\_\_\_ - руководитель;
2. \_\_\_\_\_
3. \_\_\_\_\_

3. Проверены следующие помещения:

к/

1. Кабинет руководителя предприятия.
2. Помещение бухгалтерии.

4. В ходе проверки проведены следующие работы:

1. Визуальный осмотр ограждающих конструкций, мебели и других предметов интерьера (трудозатраты - \_\_\_ чел. часов).
2. Проверка элементов строительных конструкций, мебели и других предметов интерьера с использованием специальных поисковых технических средств ( \_\_\_ чел. часов).
3. Проверка линий и оборудования силовой и осветительной электросети ( \_\_\_ чел. часов).
4. Проверка линий и оборудования абонентской телефонной сети ( \_\_\_ чел. часов).

5. Проверка линий и оборудования пожарной и охранной сигнализации ( \_\_ чел. часов).

6. Проверка радиоэфира на присутствие сигналов радиоизлучающих средств негласного съёма информации (радиомониторинг помещения) ( \_\_ чел. часов).

7. Проверка несанкционированных передач информации в диапазоне инфракрасного излучения ( \_\_ чел. часов).

8. Поиск средств негласного съёма информации, внедрённых в электронные приборы ( \_\_ чел. часов).

9. Визуальный осмотр внешних, выходящих на улицу поверхностей стен кабинета руководителя и помещения бухгалтерии ( \_\_ чел. часов).

10. Визуальный осмотр и проверка элементов строительных конструкций, проводных и технологических коммуникаций в соседних с проверяемыми помещениями ( \_\_ чел. часов).

5. В ходе проверки использовалась следующая поисковая и исследовательская аппаратура:

1. Комплект досмотровых зеркал ШМЕЛЬ-2 (№ \_\_ ).

2. Комплект луп, фонарей.

3. Гибкий технический эндоскоп дистальный МконцомЭТ-4-0,5АП (зав. № \_\_ ).

4. Досмотровый селективный металл оискатель УНИСКАН 7215 (зав. № \_\_ ).

5. Прибор нелинейной радиолокации NR-900ЕМ (зав. № \_\_ ).

6. Переносный флуороскоп ФП- 1 (зав. № \_\_ ).

7. Многофункциональный поисковый прибор ПИРАНЬЯ (зав. № \_\_ )

8. Низкочастотный нелинейный детектор проводных коммуникаций ВИЗИР (зав. № \_\_ ).

9. Комплекс обнаружения радиоизлучающих средств и радиомониторинга КРОНА-6000М (зав. № \_\_ ).

10. Обнаружитель скрытых видеокамер IRIS VCF-2000 (зав. № \_\_ ).

II. Дозиметр поисковый (прибор радиационного контроля) РМ-1401 (зав. № \_\_ ).

б. Результаты проверки:

1. В кабинете руководителя обнаружено подслушивающее устройство с передачей перехватываемой акустической информации по проводам силовой электрической сети. Устройство на момент проверки работоспособно, выполнено в виде тройника-разветвителя и подключено к розетке электрической сети возле рабочего стола руководителя предприятия. Радиус съёма акустической информации - около шести метров, дальность передачи перехватываемой информации - до силового трансформатора, размещённого в электросиловой будке, находящейся за пределами охраняемой территории.

Наиболее вероятные места съёма передаваемой информации: электророзетки в приёмной, коридоре, подсобных помещениях и туалетной комнате, электросилового щита на лестничной площадке, электросиловая будка за пределами предприятия. Вероятное время установки - (дата) \_\_\_\_, во время проведения ремонта кабинета. ^

Обнаруженное подслушивающее устройство нейтрализовано путём акустической изоляции микрофона и оставлено на месте обнаружения.

Других средств негласного съёма информации в кабинете руководителя не обнаружено.

2 В помещении бухгалтерии средств негласного съёма информации не обнаружено.

3. Кабинет руководителя предприятия недостаточно защищён от утечки защищаемой информации по техническим каналам:

1. возможна утечка акустической информации через канал естественной вентиляции помещения;

2. возможна утечка акустической информации через виброакустический канал, образованный магистралью парового отопления;

3. возможен несанкционированный съём информации с монитора компьютера путём перехвата его ПЭМИ.

Помещение бухгалтерии не защищено от утечки защищаемой информации по техническим каналам:

1. возможна утечка акустической информации через тонкую дверь и гипсокартонную часть перегородки с помещением приёмной;

2. возможна утечка акустической информации через канал естественной вентиляции помещения;

3. возможна утечка акустической информации через виброакустический канал, образованный магистралью парового отопления;

4. существует возможность дистанционного, без подключения дополнительных устройств перехвата телефонных переговоров, ведущихся с радиотелефона PANASONIC;

5. возможен несанкционированный съём информации с мониторов компьютеров и другой оргтехники путём перехвата ПЭМИ;

6. возможна утечка информации, снимаемой визуально или с использованием фото- и видеотехники, через незашторенное окно и застеклённую часть входной двери.

Оба помещения не защищены от несанкционированной записи конфиденциальных переговоров на диктофон, съёмки скрытыми видеокамерами и возможной утечки информации за счёт наводок в проводных линиях, проложенных параллельно проводам телефонной сети. Помещения имеют много мест, удобных для подброса радиомикрофонов или быстрой установки других видов средств негласного съёма информации.

7. Рекомендации по повышению защищённости проверенных помещений

и предотвращению утечки информации по выявленным техническим каналам её утечки изложены в отдельном документе.

*Руководитель поисковой бригады*

Л : . . ■ .. \_\_\_\_\_ / \_\_\_\_\_ / ;

■ -,;,; ■ Члены бригады: ;

■ '■ ■ ' ■ ..... У \_\_\_\_\_ / \_\_\_\_\_ / \*

1

: " \_ " \_\_\_\_\_ 200\_г.

**Приложение 7.**

**Отчёт, формируемый комплексом КРОНА-6000М (вариант).**

КОНФИДЕНЦИАЛЬНО

ЭКЗ.№ 1

ОТЧЕТ О РАБОТЕ 24.08.00

Начало работы : 10:21:12  
Окончание работы : 10:41:11

Объект проверки : кабинет генерального директора  
Оператор : Иванов И.И.

В процессе работы проверялся диапазон частот  
от 30.000 до 6000.000 МГц

Применялись следующие тесты:  
ВНЕШНИЙ ПАССИВНЫЙ  
ВНЕШНИЙ АКТИВНЫЙ TV  
СИГНАЛА ЦИФРОВОГО  
СИГНАЛА

В результате поиска-найдено сигналов: 251. Из  
них:

. 1 - обнаруженные закладки , . ■ , ■ ■  
.....





Приложение 8.

**Рекомендации по повышению защищённости помещений и объектов (вариант).**

Конфиденциально

Экз. № \_  
Всего \_ экз.

Рекомендации по повышению  
защищённости помещений

*1. Перечень выявленных в проверенных помещениях потенциальных технических каналов утечки информации (ТКУИ):*

1. Кабинет руководителя предприятия:

1. акустический воздушный ТКУИ через канал естественной вентиляции помещения;
- 2 акустический вибрационный ТКУИ через канал естественной вентиляции помещения;
3. акустический вибрационный ТКУИ через магистраль (трубопровод) парового отопления помещения;
- 4 электромагнитный ТКУИ за счёт перехвата ПЭМИ монитора компьютера;
5. электрические ТКУИ за счёт съёма наводок с проводных линий пожарной и охранной сигнализации, проложенных параллельно проводам телефонной линии.

6. Помещение бухгалтерии:

1. акустический воздушный ТКУИ через канал естественной вентиляции помещения;
- 2 акустический воздушный ТКУИ через входную дверь помещения;
3. акустический воздушный ТКУИ через гипсокартонную перегородку с помещением приёмной;
- 4 акустический вибрационный ТКУИ через канал естественной вентиляции помещения;
5. акустический вибрационный ТКУИ через гипсокартонную перегородку с помещением приёмной;
6. акустический вибрационный ТКУИ через магистраль (трубопровод) парового отопления помещения;
7. электромагнитные ТКУИ за счёт перехвата ПЭМИ мониторов компьютеров и другой оргтехники;

8. электрические ТКУИ за счёт съёма наводок с проводных линий пожарной и охранной сигнализации, проложенных параллельно проводам телефонной линии;

9. возможна утечка информации за счёт прямого перехвата сигнала радиотелефона PANASONIC;

Ю. возможна утечка информации, снимаемой визуально или с использованием фото- и видеотехники, через незашторенное окно и застеклённую часть входной двери.

Оба помещения не защищены от несанкционированной записи на диктофон, съёмки скрытыми видеокамерами и подброса радиомикрофонов.

Схемы выявленных потенциальных ТКУИ с краткими пояснениями (легендами) - в приложении № 1 к документу<sup>7</sup>.

## **2. Оценка вероятности использования противником потенциальных ТКУИ и защищённости помещений:**

### **1. Кабинет руководителя предприятия:**

Ввиду хорошей слышимости и разборчивости речевых сигналов и доступности для противника соседних помещений вероятности использования противником акустического воздушного и акустического вибрационного потенциальных ТКУИ можно считать *высокими*.

Использование противником акустического вибрационного ТКУИ через магистраль (трубопровод) парового отопления из-за слабой разборчивости сигналов можно считать *вероятным*.

Использование противником электромагнитного ТКУИ за счёт перехвата ГОМИ монитора компьютера и электрического ТКУИ за счёт съёма наводок с проводных линий можно считать *маловероятным*, но возможным. В связи с отсутствием в кабинете специальных средств защиты информации от её утечки по выявленному потенциальному ТКУИ и высокой вероятностью использования противником акустического воздушного и акустического вибрационного потенциальных ТКУИ кабинет руководителя предприятия следует считать *незащищённым* от утечки защищаемой информации по техническим каналам.

### **2 Помещение бухгалтерии:**

*(далее даётся оценка вероятности использования противником потенциальных ТКУИ и оценка защищённости помещения от негласного съёма информации)*

## **3. Рекомендации по мерам и способам предотвращения съёма информации по выявленным потенциальным ТКУИ и повышению защищённости помещений:**

i. Кабинет руководителя предприятия:

1. Для защиты помещения от утечки акустической информации через канал естественной вентиляции помещения рекомендуется зашумление канала путём создания акустических и вибрационных помех с помощью генератора акустического шума. Наиболее эффективной системой защиты является комплекс виброакустической защиты БАРОН. Частичной, более дешёвой альтернативой (когда невозможно установить генератор акустического шума АКО-2000).

Эти же средства обеспечат защиту помещения от утечки акустической информации через магистраль (трубопровод) парового отопления и ограждающие кабинет строительные конструкции.

2. Для защиты помещения от утечки информации за счёт перехвата ПЭМИ монитора компьютера рекомендуется электромагнитное зашумление помещения с помощью генератора шума ГРОМ-ЗИ-4. Применение этого генератора обеспечит также создание помех для несанкционированного съёма информации с электрической сети, что предотвратит утечку информации в случае повторного использования противником подслушивающего устройства, аналогичного найденному в ходе проверки. В качестве альтернативы генератору шума ГРОМ-ЗИ-4 по электромагнитному зашумлению помещения может рассматриваться генератор шума ГНОМ-3 или ГШ-К-1000.

3. Для предотвращения утечки информации за счёт съёма наводок с проводных линий пожарной и охранной сигнализации рекомендуется перепрокладка телефонной линии для устранения её совместного параллельного пробега с линиями пожарной и охранной сигнализации. Альтернативой перепрокладке телефонной линии является установка в шахтах пожарной и охранной сигнализации помехоподавляющих фильтров ФП-7.

4. Для защиты помещения от несанкционированной аудиозаписи рекомендуется применение подавителя радиоэлектронных устройств негласной аудиозаписи ШТОРМ.

5. Для своевременного обнаружения несанкционированной видеосъёмки рекомендуется установка в кабинете обнаружителя скрытых видеокамер Iris VSF-2000.

2 Помещение бухгалтерии:

1. Для защиты помещения от утечки акустической информации...

*(далее даются рекомендации по мерам и способам предотвращения съёма информации по выявленным ТКУИ и повышению защищённости помещения бухгалтерии)*

**4. Сводный перечень технических средств и систем защиты информации, рекомендуемых для повышения защищенности помещений:**

Помещение	№ п/п	Рекомендуемое средство	Альтернативное средство	Назначение	Требуемое количество	
		Комплекс виброакустической защиты БАРОН	Генератор акустического шума АБЬе-2000	Защита помещений от утечки акустической информации через канал естественной вентиляции, трубопровод отопления, ограждающие строительные конструкции		
		Генератор шума ГРОМ-ЗИ-4	Генератор шума ГНОМ-Э или ГШ-К-1000 (защиту электрической сети не обеспечивают)	Защита помещения от утечки информации за счёт перехвата ПЭМИ компьютера и съёма информации с электрической сети		
		Помехоподавляющий фильтр 4>П-		Предотвращение утечки информации за счёт съёма наводок с проводных линий пожарной и охранной сигнализации		
		Подавитель радиоэлектронных устройств негласной аудиозаписи ШТОРМ		Защита помещения от санкционированной записи на диктофон		
		Обнаружитель скрытых видеокамер IRIS VSF-2000	Нет аналогов	Своевременное обнаружение несанкционированной видеосъёмки в помещении		
II		(далее продолжается перечень технических средств и систем защиты информации, рекомендуемых для повышения защищенности помещения бухгалтерии)				
	12	обнаружения радионизлучающих средств и радиомониторинга КРОНА-6000М	Мноофункциональный комплекс радиоконтроля КРК-4	Оборудование пункта радиоконтроля для постоянного (круглосуточного) радиомониторинга служебных помещений		
	13	Многоканальный цифровой магнитофон ГЛУХАРЬ		Обеспечение гласного санкционированного контроля акустики служебных помещений и установленных руководством ограничений на использование телефонных каналов связи		
	14					

**5. Предложения по практическому использованию рекомендуемых средств и систем защиты информации:**

I. Комплекс виброакустической защиты БАРОН способен обеспечить одновременную защиту всех проверенных помещений.

В кабинете руководителя предприятия целесообразно установить одно устройство контроля эффективности вибрационных помех БАРОН-Кишеть виброгенераторов типа БАРОН: по одному в каждом вентиляционном канале,

по одному на стекло окна, на трубопровод парового отопления, оалку потолочного перекрытия и на плиту перекрытия между вторым и третьим этажами.

В помещении бухгалтерии целесообразно установить четыре виброгенератора типа БАРОН и одно устройство контроля эффективности вибрационных помех БАРОН-К. Рекомендуемые места установки отражены на схеме приложения №2.

Установку основного блока (генератора) комплекса виброакустической защиты устройства дистанционного включения виброгенераторов БАРОН-В рекомендуется провести в помещении службы безопасности.

Включение помехового сигнала в защищаемых помещениях рекомендуется осуществлять из помещения службы безопасности на время ведения конфиденциальных переговоров. Контроль эффективности помех целесообразно осуществлять по сигналу тревоги, подаваемому устройствами БАРОН-К, установленными в защищаемых помещениях.

2 Генераторы шума ГРОМ-ЗИ-4 рекомендуется установить по одному в каждом защищаемом помещении.

Включение электромагнитного зашумления помещения в кабинете руководителя предприятия целесообразно осуществлять на время работы с ПЭ ВМ, в помещении бухгалтерии - с началом рабочего дня.

Включение режима линейного зашумления электросети рекомендуется с началом рабочего дня, выключение - по его окончании.

Режим защиты телефонной линии генератора шума ГРОМ-ЗИ-4 в кабинетеруководителя предприятия использовать не рекомендуется в связи с применением для этой цели более эффективного устройства защиты ПГОКРУСТ-2000.

3. Установку помехоподавляющих фильтров ФП-7 в линий пожарной и охранной сигнализации защищаемых помещений рекомендуется осуществить согласно схемам приложения №2.

4 Подавитель радиоэлектронных устройств негласной аудиозаписи ШТОРМ рекомендуется включать с помощью пульта дистанционного управления на время проведения совещаний и конфиденциальных переговоров.

(далее продолжаютя предложения по практическому использованию средств и систем защиты информации, рекомендованных для повышения защищённости помещений)

**Приложения** (не прилагаются) j

1. Схемы выявленных по результатам проверки потенциальных технических каналов утечки информации.
2. Схемы установки рекомендуемых средств и систем защиты

*Согласовано*

Руководитель организации,  
проводящей проверку

Руководитель поисковой бригады

\_\_\_\_\_ / \_\_\_\_\_ /

Члены поисковой бригады

\_\_\_\_\_

\_\_\_\_\_

200\_г.

" \_ " \_\_\_\_\_ 200\_г.

" \_ " \_\_\_\_\_ 200 г.

Список использованной литературы:

1. Защита информации. Основные термины и определения. ГОСТ Р 50922-96, дата введения 1997-07-01. -М.: Госстандарт России.
2. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. ГОСТ Р 51275-99, дата введения 2000-01-01.-М.: Госстандарт России.
3. Хорев А.А. Способы и средства защиты информации.-М.:МОРФ. 1998. -316с.
4. Пятачков А. Г. Рекомендации по защите информации от утечки по техническим каналам на объектах информатизации. //Защита информации «Конфидент». 1999. №4-5.
5. Положение о государственном лицензировании деятельности в области защиты информации. (Решение Гостехкомиссии России и ФАПСИ от 27.04.94 г. №10).
6. Положение о государственном лицензировании деятельности в области защиты информации. (Решение Гостехкомиссии России и ФАПСИ от 24.06.97г. №60).
7. Положение о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от её утечки по техническим каналам. Постановление Совета Министров - Правительства РФ от 15.09.93г. №912-51.
8. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Гостехкомиссия России. 1992.
9. Поздняков Е. Н. Защита объектов (рекомендации для руководителей и сотрудников служб безопасности). -М.: Концерн «Банковский Деловой Центр». 1997.-224 с.
10. Методологические основы обеспечения информационной безопасности объекта. // Защита информации «Конфидент». 2000. № 1. С. 75-86.
11. Справочник по радиоконтролю. Международный Союз Электросвязи. 1995.-442 с.
12. Алексеенко В. Н., Ковалёв Ю. Радиомониторинг в системе обеспечения безопасности коммерческих объектов.-М.: РоссиСекьюрити, 1997. -43 с.
13. Портативный сетевой металлодетектор «Унискан 7215». Руководство пользователя.- М.: АКА, 1999.
14. Джонс Т. Обзор технологии нелинейной локации. // Системы безопасности, связи и телекоммуникаций. 1999. № 26. С. 34-36.
15. Гавриш В. А. Практическое пособие по защите коммерческой тайны. - Симферополь: Таврида, 1994. -112 с.
16. Лысов А. В. Общая характеристика портативных средств акустической



- разведки. // Безопасность информационных технологий. 1995. №2.
17. Петраков А. В. Основы практической защиты информации. -М.: Радио и связь, 1999.-368 с.
  18. Петраков А. В., Лагутин В. С. Утечка и защита информации в телефонных каналах. -М.: Энергоатомиздат, 1998.-320 с.
  19. Хорев А. А. Технические средства и способы промышленного шпионажа. -М.: 1997.-230 с.
  20. Халяпин Д. Б., Ярочкин В. И. Основы защиты информации. Учебное пособие.-М.: ИПКИР, 1994.-125 с.
  21. Лысов А В., Остапенко А. Н. Телефони безопасность. (Проблемы защиты информации в телефонных сетях.)-СПб.: 1995.- 105 с.
  22. Хорев А. А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. Учебное пособие. - М.: Гостехкомиссия России, 1998. - 320 с.
  23. Шаповалов П. П. Практическое руководство по поиску устройств съёма и передачи информации. М.: ЗАО «Щит», 1997. - 52 с.
  24. Регламент радиосвязи//Системы безопасности. 1995.№5.

## ХОЛДИНГ ПРЕДПРИЯТИИ БЕЗОПАСНОСТИ "НЕЛК"

Осуществляет свою деятельность в области обеспечения комплексной безопасности бизнеса и личности по следующим направлениям:

- Проведение научно-исследовательских и опытно-конструкторских работ для совершенствования существующих и создания новых технологий в области радиоконтроля и защиты информации от утечки по техническим каналам.
- Разработка средств защиты информации от утечки по техническим каналам.
- Создание программно-аппаратных комплексов радиоконтроля в интересах различных ведомственных организаций.
- Проведение технических и организационных мероприятий по защите информации от разведки с использованием специальных технических средств и от ее утечки по техническим каналам, инструментальные оценки возможных каналов утечки информации из технических средств, объектов и помещений.
- Создание и внедрение комплексных систем безопасности, включающих в себя: разработку концепции безопасности; математическое моделирование эффективности системы безопасности; системы наружного, внутреннего и скрытого теленаблюдения, с передачей видеозображения как по проводным, так и по радиоканалам; системы контроля доступа; системы охранно-пожарной сигнализации; системы охраны периметра.
- Обучение в Учебном центре по программам подготовки руководителей и специалистов служб безопасности.
- Охрана имущества собственника<sup>^</sup> т.ч. при транспортировке.
- Разработка концепции и проведение консультаций по вопросам обеспечения комплексной безопасности объекта по направлениям:
  - информационная безопасность (порядок документооборота на бумажных носителях, порядок документооборота на электронных носителях, анализ и рекомендации по размещению сотрудников по помещениям и оборудованию их техническими средствами защиты от утечек информации по техническим каналам);
  - технические средства охранно-пожарной сигнализации;
  - пожарная безопасность;
  - правомерная защита от противоправных посягательств;
  - экспертиза объектов на предмет технической защищенности и организационных мер обеспечения безопасности;
  - рекомендации по функциональному назначению помещений (офисов) с точки зрения обеспечения безопасности;
  - оказание консультационных услуг по выбору оборудования обеспечения безопасности и связи.

### **В состав Холдинга предприятий безопасности "НЕЛК" входят:**

- Закрытое акционерное общество **Научно-производственный центр "НЕЛК"**;
- Закрытое акционерное общество **Частное охранное предприятие "НЕЛК-ГАРД"**;
- Негосударственное образовательное учреждение **Научно-информационный центр "НЕЛК"**.

# НАУЧНО-ИНФОРМАЦИОННЫЙ ЦЕНТР "НЕЛК"

НОУ НИЦ "НЕЛК" образовано в 2000 году (лицензия Комитета образования г. Москвы № 003388 от 12 июля 2000 года, регистрационный номер 006452). Одной из основных задач Научно-информационного центра является подготовка, переподготовка и повышение квалификации специалистов, работающих в сфере защиты информации от несанкционированного доступа и обеспечения безопасности предпринимательской деятельности. За это время в нашем Центре прошли обучение более 300 руководителей и ведущих специалистов подразделений по защите информации предприятий, учреждений и организаций различных форм собственности. Занятия проводят ведущие специалисты Минобороны, Российского государственного гуманитарного университета, Московского инженерно-физического института, представители фирм-разработчиков техники защиты информации и Научно-производственного центра "НЕЛК". Большинство преподавателей имеют ученые степени и звания.

Программы обучения имеют различную тематику, предназначение и продолжительность и организуются по следующим направлениям:

**1. "Организация комплексной защиты информации на предприятиях, в учреждениях и организациях"** - продолжительность обучения 80 часов (10 учебных дней) с выдачей удостоверения государственного образца о краткосрочном повышении квалификации.

**2. "Защита информации от утечки по техническим каналам. Новинки рынка защиты информации" (базовый курс)** - продолжительность обучения 40 часов (5 учебных дней) с выдачей удостоверения установленного образца о краткосрочном повышении квалификации.

**3. "Методика, технические средства обнаружения и противодействия устройствам съема конфиденциальной информации. Устройства комплексной защиты и основы их применения"** - продолжительность обучения 24 часа (3 учебных дня).

**4. "Комплексное обеспечение безопасности предпринимательской деятельности"** - обзорный курс для руководителей предприятий и организаций, начальников служб безопасности (6 часов).

Для всех учебных программ базовыми являются следующие темы:

- государственная система и нормативно-правовая база защиты информации в РФ;
- физические принципы возникновения технических каналов утечки информации;
- организация и методика проведения защитно-поисковых мероприятий;
- технические системы защиты информации и основы их применения.

Для слушателей организуются:

- Консультации специалистов по интересующим темам.

• Индивидуальные практические занятия с интересующей техникой защиты информации.

- Бесплатное обеспечение учебно-методическими материалами.

• Индивидуальная адаптация учебной программы к практическим потребностям слушателя по изучению техники защиты информации.

- Бесплатные обеды.

*Прошедшим обучение предоставляется 3% скидка от стоимости техники и программных продуктов, разрабатываемых НПЦ "НЕЛК".*

*Форма оплаты за обучение любая. Действует гибкая система скидок.*



Частное охранное предприятие  
«НЕЛК – ГАРД»

Главное отличие "НЕЛК-ГАРД" от большинства подобных предприятий в том, что основной своей задачей мы видим не выставление охранного объекта, а обеспечение его безопасности и повышения эффективности работы объекта. При подготовке объекта под охрану мы проводим экспертизу объекта по направлениям:

Техническая укрепленность объекта - наличие и качество заборов, ограждений, решеток, дверей и их запорных устройств, вентиляционных и коммуникационных шахт, правильность оборудования кассовых узлов, сейфовых комнат, помещений для хранения ценностей и т.д.

Техническая оснащенность объекта - наличие и качество средств ОПС (Охранно-Пожарной Сигнализации), охранного ТВ, СКД (Системы Контроля Доступа), офисной АТС, ЛВС (Локальной Вычислительной Сети), систем автоматизации и мониторинга зданий (сооружений).

Пожарная безопасность объекта - соответствие объекта и его оснащенность средствами первичного пожаротушения требованиям ППБ (Правил Пожарной Безопасности).

Режим объекта - порядок входа/выхода и регистрации сотрудников, посетителей, сотрудников государственных контролирующих органов, порядок закрытия/открытия, как объекта в целом, так и отдельных помещений, порядок готовности к действиям персонала в различных нестандартных ситуациях и т.п.

Информационная безопасность - наличие ограничений доступа к информации, представляющей коммерческую тайну, порядок доступа, хранения и уничтожения носителей данной информации, подключение к ИНТЕРНЕТУ защищенного санкционированного доступа, наличие технических каналов утечки информации и защиты от них.

**Наше кредо** - не просто ставить вопросы, а решать их и работать на предупреждение кризисных ситуаций.

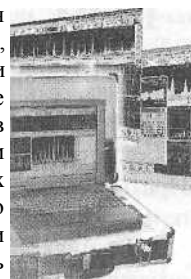
**Наша задача** - обеспечить безопасность и повысить эффективность Вашей работы с максимальным использованием уже имеющихся у Вас ресурсов.

**Наш подход** - не отнимать время у руководства Заказчика, а по максимуму разгрузить его для решения основных производственных задач.

---

## Комплекс обнаружения радиоизлучающих средств и радиомониторинга КРОНА-6000М

Предназначен для автоматического обнаружения радиоизлучающих устройств (акустических закладок), скрытых видеокамер независимо от способа передачи видеосигнала, работающих диктофонов (в том числе цифровых) и определения их местоположения в контролируемом помещении. С высоким быстродействием определяет частоты и уровни любых радиосредств в диапазоне до 6 ГГц, распознает скрытно установленные в помещении радиомикрофоны и определяет расстояние до них. Имеет возможность автоматической классификации цифровых каналов передачи данных, что существенно облегчает обнаружение цифровых радиозакладок.



Разработан на основе анализа недостатков существующих поисковых систем и представляет собой реализацию новой концепции создания автоматизированных поисковых программно-аппаратных комплексов. Выгодно отличается от них бесшумностью работы, улучшенным дизайном, большей степенью автоматизации, модульным принципом построения и сравнительно низкой стоимостью при существенно больших технических возможностях. Поисковые показатели и круг решаемых задач существенным образом зависят от программного обеспечения, которое динамично развивается. Параллельно готовится к выпуску широкая номенклатура аппаратных опций.

Комплекс работает под управлением универсального поискового программного обеспечения ФИЛИН, реализующего все известные к настоящему времени алгоритмы обнаружения подслушивающих устройств. В программе реально воплощен принцип полной автоматизации работы аппаратуры: "включил-получил результат".

При автоматизированном радиоконтроле осуществляется запись на жесткий диск ПЭВМ панорамы загрузки, демодулированных речевых сигналов, их несущих частот, осциллограмм, корреляционных функций, времени обнаружения, длительности и относительного уровня сигналов с возможностью их последующей обработки. Возможно проведение детального анализа принимаемых сигналов оператором по их спектральным составляющим, осциллограммам, корреляционным функциям и другим характеристикам.

НАУЧНО-ПРОИЗВОДСТВЕННЫЙ ЦЕНТР "НЕЛК"  
109377, Россия, Москва,  
1-ая Новокузьминская улица, дом 8/2  
тел.: +7-(095)174-9264, 174-9168,  
174-9842, 378-2111  
Интернет: <http://www.nelk.ru> E-  
mail: [nelk@aha.ru](mailto:nelk@aha.ru)

## Обнаружитель скрытых видеокамер IRIS VCF-2000

В последнее время в области технического шпионажа все шире применяются миниатюрные видеокамеры. Полученные с их помощью видеоматериалы в дальнейшем нередко используются при шантаже, вымогательстве, выбросах компромата и других противоправных действиях.

Достижения в области миниатюризации позволяют разместить современную шпионскую видеокамеру практически в любых предметах интерьера и личных вещах. Очень сложно разглядеть электронное око с диаметром отверстия меньше миллиметра в узоре галстука собеседника, настенных часах или картине. Подобная техника делает возможным контроль над человеком в тех ситуациях, где он и не подозревает о наличии чужого взгляда.

Сегодня задача обнаружения скрытых видеокамер приобретает все большую значимость. Последние модели микрокамер по своим габаритным и техническим характеристикам приближаются к традиционным средствам шпионажа (диктофоны, радиомикрофоны-жучки). Вместе с тем обнаружить скрытую видеокамеру гораздо сложнее других способов утечки информации, и до недавнего времени являлось почти невыполнимой задачей.

Появление прибора автоматического обнаружения видеокамер АЙРИС явилось сенсацией на рынке технических средств безопасности. Специалисты пожимают плечами и удивленно констатируют, что ничего подобного не встречали. Действительно, небольшой прибор размером меньше автомагнитолы способен за недолгий промежуток времени обнаружить работающую шпионскую видеокамеру на расстоянии до 5-ти метров. Но самое главное, теперь не требуется специальных навыков и проведения отдельных поисковых мероприятий. Необходимо лишь включить прибор в подозрительном помещении и дождаться результата. Устройством автоматическом режиме проверяет обстановку на наличие работы большинства типов используемых сегодня микровидео-камер. В случае обнаружения подозрительного источника есть возможность определить его местоположение с помощью встроенного индикатора интенсивности.

Благодаря небольшим габаритам и простоте применения обнаружитель АЙРИС может использоваться в различных ситуациях и без выдачи своих намерений. По совокупности характеристик данная разработка сегодня не имеет аналогов во всем мире.

Обеспечит  
конфиденциальность  
Ваших переговоров,  
отдыха и т.н.



Просто нажмите кнопку!

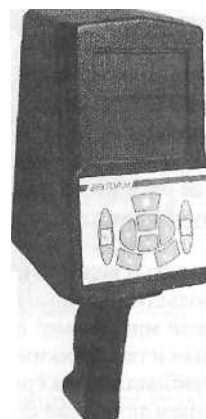
125

НАУЧНО-ПРОИЗВОДСТВЕННЫЙ ЦЕНТР "НЕЛК"  
109377, Россия, Москва, 1-ая  
Новокузьминская улица, дом 8/2 тел.:  
+7-(095) 174-9264, 174-9168, 174-  
9842, 378-2111 Интернет:  
http://www.nslk.ru E-mail: nelk@aha.ru

## Восьмиканальный индикатор электромагнитных излучений ВЕКТОР

Может быть успешно использован для решения как исследовательских, так и прикладных задач специального назначения, в том числе:

- для обнаружения и локализации специальных технических средств негласного получения информации (закладных устройств), функционирующих в СВЧ диапазоне;
- для обнаружения внедренных закладных устройств (размещенных в различных технических средствах), функционирующих в СВЧ диапазоне;
- для обнаружения и локализации источников не преднамеренных помех в СВЧ диапазоне;
- для оценки общей фоновой обстановки в СВЧ диапазоне;
- для обнаружения аномалий в СВЧ диапазоне в части контроля биологической безопасности и т. д.



### *Технические характеристики:*

- Рабочий диапазон частот: 2...18 ГГц.
- Тип приемных антенн: Z-образная; щелевая.
- Поляризация антенн: 45 град.
- Коэффициент усиления антенн:
  - в диапазоне 2...8 ГГц - не менее 5 дБ;
  - в диапазоне 8...18 ГГц - не менее 4 дБ.
- Чувствительность приемных каналов: не хуже -70 дБ/Вт;
- Динамический диапазон: не менее 30 дБ/Вт.

Особенностью индикатора является большой диапазон рабочих частот при достаточно высоких характеристиках приемного тракта. Применение цифровой обработки позволило значительно повысить оперативность и удобство при эксплуатации. Возможность размещения индикатора стационарно (натреного) и передавать данные на внешний компьютер позволяют организовать долговременный мониторинг интересующей области пространства или объекта.

НАУЧНО-ПРОИЗВОДСТВЕННЫЙ ЦЕНТР "НЕЛК"  
109377, Россия, Москва,  
1-ая Новокузьминская улица, дом 8/2  
тел.: +7-(095) 174-8264, 174-9168,  
174-9842, 378-2111  
Интернет: <http://www.nelk.ru>  
E-mail: [nelk@aha.ru](mailto:nelk@aha.ru)

## Персональные и поисковые дозиметры

### Персональный дозиметр РМ-1203

Предназначен для измерения эквивалентной дозы и мощности эквивалентной дозы гамма-излучения.



Имеет малые размеры и вес, низкое энергопотребление, звуковую сигнализацию о превышении устанавливаемых порогов по мощности дозы и дозе, встроенные электронные часы.

Детектор - газоразрядный счетчик. Диапазон энергий гамма-излучения - 0,060 -1,5 МэВ. Диапазон измерения мощности эквивалентной дозы 0,10 505 мкЭв/ч, эквивалентной дозы - 0,001 9999 мЗв. Время измерения 1 36 с. Время непрерывной работы с одним комплектом элементов питания типа V357 один год.

### Дозиметр гамма-излучения наручный РМ-1603

Предназначен для измерения амбиентной эквивалентной дозы и мощности амбиентной эквивалентной дозы гамма-излучения с выводом результатов измерений на ЖКИ. Имеет звуковую сигнализацию при превышении



установленных порогов по дозе и мощности дозы; запоминание в энергонезависимой памяти индивидуального кода пользователя и 1000 событий истории накопления дозы в формате, определяемом пользователем; возможность обмена информацией через ИК -канал связи между дозиметром и персональным компьютером; герметичный ударопрочный корпус; малые габариты и массу; многофункциональные электронные часы с будильником,

таймером и секундомером; электролюминесцентной подсветкой ЖКИ. Детектор: счетчик Гейгера-Мюллера. Диапазон измерения мощности дозы: 0,001 - 5000 мЭв/ч. Диапазон измерения дозы: 0,001 - 9999 мЭв.

### Дозиметр индивидуальный РМ-1620



Предназначен для измерения индивидуальной эквивалентной дозы и мощности индивидуальной эквивалентной дозы гамма и рентгеновского излучения с выводом результатов измерения на ЖКИ.

Имеет звуковую сигнализацию при превышении установленных порогов по дозе и мощности дозы; запоминание и сохранение в энергонезависимой памяти индивидуального кода пользователя и 1000



событии истории накопления дозы в формате, определяемом пользователем; возможность обмена информацией через ИК-канал связи между дозиметром и персональным компьютером; малые габариты и массу; электролюминесцентную подсветку ЖКИ. В дозиметр может быть дополнительно установлен ТЛ-детектор для измерения дозы при импульсных излучениях, в аварийных ситуациях. Детектор: счетчик Гейгера-Мюллера. Диапазон мощности эквивалентной дозы: 0,0001 - 200 мЭв/ч. Диапазон измерения эквивалентной дозы: 0,001 - 9999 мЭв.

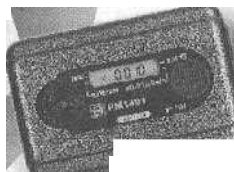
#### Дозиметр поисковый микропроцессорный РМ-1401

Предназначен для обнаружения и локализации источников гамма-излучения в полевых условиях и измерения мощности эквивалентной дозы гамма излучения. Обладает повышенной чувствительностью к оружейным материалам. Дозиметр разработан для жестких условий эксплуатации и рекомендуется сотрудникам таможенных, пограничных и аварийных служб, гражданской обороны, пожарной охраны, полиции, военных ведомств. Прибор прочен к падению с высоты 0,7 м на бетонный пол, устойчив к воздействию соляного тумана. Обнаруживает сверхмалые количества радиоактивных и ядерных материалов. Детектор: скintиллятор CsI(Tl). Время измерения: 0,25 с.




#### Дозиметр-радиометр поисковый микропроцессорный РМ-1402

Предназначен для обнаружения и локализации источников гамма-излучения в полевых условиях и измерения мощности эквивалентной дозы гамма излучения. Обладает повышенной чувствительностью к оружейным материалам. Дозиметр разработан для жестких условий эксплуатации и рекомендуется сотрудникам таможенных, пограничных и аварийных служб, гражданской обороны, пожарной охраны, полиции, военных ведомств. Прибор прочен к падению с высоты 0,7 м на бетонный пол, устойчив к воздействию соляного тумана.



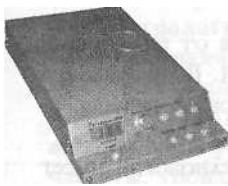
Детекторы альфа, бета, гамма, нейтронного излучений. Поиск, локализация и экспресс идентификация радиоактивных и ядерных материалов. Звуковая сигнализация и наручный вибрационный сигнализатор для скрытного обнаружения. 512-канальный анализатор для экспресс гамма спектрометрии с запоминанием ПО спектров. Порт К8-232 для передачи данных в компьютер.

 НАУЧНО-ПРОИЗВОДСТВЕННЫЙ ЦЕНТР "НЕЛК"  
109377, Россия, Москва, 1-ан  
Нонокозьминская улица, дом 8/2 тел.:  
+7-(095) 174-3254, 174-9163, 174-  
5122, 378-2111 Интернет:  
<http://www.nelk.ru> E-mail: [nelk@aha.ru](mailto:nelk@aha.ru)

## Комплексная защита телефонных линий приборами марки "ПРОКРУСТ"

- Подавление нормальной работы телефонных закладок любых типов подключения
- Гарантированное блокирование работы комбинированных радиопередатчиков и закладок типа "телефонное ухо"
- Блокировка проникновения сигналов от аппаратуры ВЧ-навязывания
- Возможность создания участка повышенной защищенности
- Встроенное стробирующее устройство управлением напряжением и током на телефонной линии
- Обеспечение ложного фактивания звукозаписывающей аппаратуры СНсгМЫVOX(VOR)
- Гарантированное определение и индикация параллельного телефона
- Возможность блокировки пиратских телефонов, подключенных к линии

**ПРОКРУСТ-2000** - Устройство защиты телефонных переговоров от прослушивания и записи. Максимальная защита линии (от телефонного аппарата до АТС) Режимы работы: детектор, помеха, уровень, стробирование, блокировка. Организуется участок дополнительной защищенности для гарантированного предотвращения снятия и передачи информации по тел. линии при положенной трубке. Возможность дистанционного управления, включение одной кнопкой, световая индикация пиратского использования линии в промежутках между переговорами, подключение звукозаписывающих устройств для документирования переговоров. Сертификат Гостехкомиссии.



**Прокруст ПТЗ-003** - устройство защиты телефонных переговоров от прослушивания и записи. Защищает телефонную линию (от аппарата до АТС) от устройств перехвата различного типа с контактным и индукционным подключением. Цифровая индикация напряжения телефонных линий, трирежима подавления (уровень, ВЧ помеха, шум), возможность подключения диктофона, светодиодная индикация. Сертификат Гостехкомиссии.



.. НАУЧНО-



ПРОИЗВОДСТВЕННЫЙ ЦЕНТР "НЕЛК"  
109377, Россия, Москва,  
1-ая Новокузьминская улица, дом  
8/2  
тел.: +7-(095) 174-9264, 174-9168,  
Интернет:  
<http://www.nelk.ru> E-mail:  
[nelk@aha.ru](mailto:nelk@aha.ru)

174-9842,378-2111

Возможность формирования помехового сигнала от различных внутренних и внешних источников и их комбинаций. Возможность подключения комплексу источников специального помехового сигнала.

Одним прибором можно защитить помещения большой площади.

Комплекс разработан с учётом новейших цифровых технологий, имеет удобный интерфейс управления и возможность подключения ПК через порт RS-232

Возможность регулировки спектра помехового сигнала для повышения эффективности наведенного помехового сигнала.

Наличие четырех независимых выходных каналов с отдельными регулировками для оптимальной настройки помехового сигнала.

Достижение максимальной эффективности подавления при минимальном паразитном акустическом шуме.

Возможность подключения к каждому выходному каналу различных типов вибро- и акустических излучателей и их комбинаций.

Модель Барон сертифицирована Госехкомиссией РФ для защиты объектов информатизации 1-ой категории.



НАУЧНО-ПРОИЗВОДСТВЕННЫЙ ЦЕНТР "НЕЛК"  
109377, Россия, Москва, 1-ая  
Новокузьминская улица, дом 8/2 тел.:  
+7.(095) 174-9264, 174-9168, 174-  
9842,378-2111 Интернет:  
<http://www.nelk.ru> E-mail: [nelk@aha.ru](mailto:nelk@aha.ru)

---

## Комплекс для проведения исследований на сверхнормативные побочные электромагнитные излучения НАВИГАТОР

Для автоматизированного измерения побочных электромагнитных излучений от проверяемых технических средств, регистрации, хранения, обработки и документирования полученных результатов.



Представляет собой автоматизированный исследовательский программно-аппаратный комплекс нового поколения. Создан на базе современных анализаторов спектра Hewlett Packard, Rohde&Schwarz, Advantest, Tektronics, Anritsu, Marconi, управляемого ПЭВМ с использованием специального про-

граммного обеспечения, разработанного фирмой «НЕЛК» с учетом действующих нормативно-методических документов Гостехкомиссии России.

### **Метрологический сертификат соответствия и сертификат Гостехкомиссии РФ.**

Программно-аппаратный комплекс позволяет:

- в автоматизированном режиме обнаруживать ПЭМИ тестируемой аппаратуры и формировать список обнаруженных ПЭМИ с регистрацией частоты, уровня ПЭМИ, полосы пропускания и антенны, при которых производилось обнаружение;
- в автоматизированном режиме верифицировать список обнаруженных ПЭМИ при включенном и выключенном тесте на исследуемой аппаратуре;
- отображать на мониторе компьютера спектры обнаруженных сигналов;
- проводить ручную верификацию списка обнаруженных ПЭМИ, используя осциллографический режим работы анализатора для наблюдения демодулированного тестового сигнала с одновременным прослушиванием теста в звуковом диапазоне частот на встроенных динамиках;
- проводить обработку полученных результатов и расчет зон разведдоступности ПЭМИ и коэффициента защищенности объекта по методикам Гостехкомиссии России;
- проводить инженерные исследования изымаемых органами МВД технических средств (радиостанций, радиомикрофонов, систем съема информации и т.д.).



НАУЧНО-ПРОИЗВОДСТВЕННЫЙ ЦЕНТР "НЕЛК"  
109377, Россия, Москва, 1-ая  
Новокузьминская улица, дом 8/2 тел.:  
+7-(095) 174-9264, 174-9168, 174-  
9842,378-2111 Интернет:  
<http://www.nelk.ru> E-mail: [netk@aha.ru](mailto:netk@aha.ru)

## Комплекс для проведения акустических и виброакустических измерений СПРУТ-5

### Назначение:

Для проведения комплекса акустических и виброакустических измерений и специальной обработки полученных результатов.

### Возможные применения:

- Измерение параметров звуко- и виброизоляционных свойств конструкций;
- Исследование характеристик и проверка эффективности систем акустического и виброакустического шумления;
- Измерение сигналов акусто-электрических преобразователей.
- Измерение электрического и магнитного поля и наводок на проводные коммуникации.
- Измерение характеристик акустических и виброакустических сигналов в во временной и частотной областях, в том числе БПФ, октавный и третьоктавный анализ, статистическая обработка и т.п.



### Достоинства:

1. Использование независимой аппаратной части, построенной на малошумящих усилителях и высокоэффективных схемах аналого-цифровой обработки сигнала, позволяет производить высокоточные измерения уровней сигналов получаемых с различных видов входных преобразователей .

2. Наличие каскадов с различным входным сопротивлением дает возможность подключать к комплексу разнообразные преобразователи (микрофон, акселерометр, токосъемник).

3. Ввиду того, что измерительный модуль обеспечивает необходимое напряжение питания для измерительных микрофонов и акселерометров (например фирмы Брюль и Кьер), они могут подключаться непосредственно к модулю без в применения специальных отдельных (и достаточно дорогих) блоков питания для входных преобразователей.

4. Применение программного обеспечения для обработки результатов и управления режимами работы измерительного модуля делает комплекс гибким и дает широкие возможности по конфигурированию под различные задачи.

5. Подключение измерительного модуля к ПЭВМ осуществляется по шине USB. Такой способ подключения обладает повышенной устойчивостью к механическим повреждениям.

6. Комплекс имеет автономное питание, что делает его мобильным и удобным в эксплуатации.

7. Совместное использование с ПАК «НАВИГАТОР» позволяет решать весь спектр задач по исследованию различных объектов, обеспечивает существенную экономию средств, по ряду параметров - не имеет альтернативы.



НАУЧНО-ПРОИЗВОДСТВЕННЫЙ ЦЕНТР "НЕЛГ"  
109377, Россия, Москва, 1-ая  
Новокузьминская улица, дом 8/2 тел.:  
+7-(095) 174-9264, 174-9168, 174-  
9842, 378-2111 Интернет:  
<http://www.netk.ru> E-mail: [nelk@3ha.ru](mailto:nelk@3ha.ru)

## Устройство противодействия радиоэлектронным средствам промышленного шпионажа ШТОРМ.



Предназначено для подавления радиоэлектронных устройств в секторе не менее 80 градусов и на расстоянии 6... 10 метров не зависимо от их ориентации в пространстве.

Обеспечивает надежную нейтрализацию в рабочей зоне:

для

• Д  
и  
к  
т

офонов;

• подслушивающих устройств - радиомикрофонов, электронных стетоскопов и др.;

- оргтехники и бытовой радиоприемной аппаратуры.

"ШТОРМ", в отличие от генераторов электромагнитного шума, благодаря своему оригинальному конструктивному исполнению и направленному действию, не мешает работе радиоэлектронных устройств (в том числе и средств связи) вне зоны подавления.

Для удобства эксплуатации прибор выполнен в атташе-кейсе (мобильный вариант) или музыкальном центре (стационарный вариант) и снабжен пультами дистанционного управления.

### *Технические характеристики:*

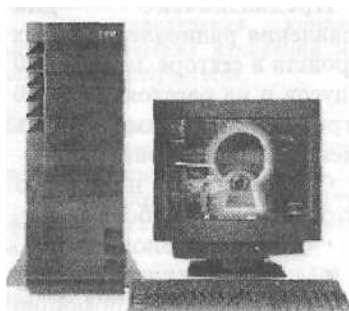
- Зона подавления - сектор с углом не менее 60 град, радиусом до 6 м по диктофонам в металлическом корпусе и до 10 м по диктофонам в пластмассовом корпусе.
- Время непрерывной работы от встроенных аккумуляторов - до 1,5 час.
- Питание - 220 В, 50 Гц.
- Потребляемая мощность - не более 60 Вт в режиме подавления.
- Габариты - 550x450x110 мм.
- Масса - не более 7 кг.

***Гигиеническое заключение Центра государственного санитарно-эпидемиологического надзора в г. Москве Министерства здравоохранения РФ.***



НАУЧНО-ПРОИЗВОДСТВЕННЫЙ ЦЕНТР "НЕЛК"  
109377, Россия, Москва, 1-ая  
Новокузьминская улица, дом 8/2 тел.:  
+7-(095) 174-9264, 174-9168, 174-  
9842, 378-2111 Интернет:  
<http://www.nelk.ru> E-mail: [nelk@aha.ru](mailto:nelk@aha.ru)

## ПАПАР АЦЦИ Программа контроля соблюдения правил работы на персональном компьютере.



Ваш персональный компьютер знает о вас очень много. Вас никогда не беспокоила мысль, что этим могут воспользоваться посторонние? Установите на компьютер ПАПАРАЦЦИ - не имеющую аналогов программу наблюдения за использованием ПК и вы будете знать наверняка - за вашей спиной не происходит ничего неожиданного! ПАПАРАЦЦИ работает абсолютно скрытно, как бы "фотографируя" изображение с экрана каждые несколько минут. Снятые кадры сжимаются, образуя фильм, который можно просмотреть в любой удобный момент.

### Какая польза от ПАПАРАЦЦИ?

Судите сами - на первой же фирме, где ПАПАРАЦЦИ был опробован, в первую же неделю был выявлен сотрудник, тайно копировавший бухгалтерские данные! Возможно, он вынашивал планы шантажа, возможно, был связан с конкурентами... Вы можете надеяться, что именно ваши сотрудники работают добросовестно, можете не обращать внимания, что при вашем появлении кто-то суетливо гасит монитор, но лучше знать наверняка - за вашей спиной не происходит ничего неожиданного.

### Как работает ПАПАРАЦЦИ?

Комплект ПАПАРАЦЦИ - это два независимо работающих модуля - "агент", который делает снимки и "монитор". Модуль "агент" устанавливается (устанавливается) на компьютер и скрытно работает на нем до удаления (деинсталляции), а "монитор" запускается с CD-ROMа каждый раз, когда нужно просмотреть накопившиеся данные или изменить настройки ПАПАРАЦЦИ - частоту кадров, удалить или сортировать их, приостановить наблюдение на любое время. Все функции просты и понятны интуитивно.

### Надежно ли защищен ПАПАРАЦЦИ?

Программа использует оригинальную методику защиты от контрнадзора, несанкционированного использования или случайного запуска. Файлы данных тщательно защищены от обнаружения и просмотра. Для пользования ПАПАРАЦЦИ нужно помнить (и сохранять в тайне) пароль и код доступа. Не зная их, воспользоваться программой или просмотреть снимки просто невозможно. И гораздо лучше, если программа работает совершенно секретно, помогая вам вовремя и надежно предупреждать любые неприятности.



НАУЧНО-ПРОИЗВОДСТВЕННЫЙ ЦЕНТР "НЕЛК"  
109377, Россия, Москва, 1-ая  
Новокузьминская улица, дом 8/2 тел.:  
+7-(095) 174-9264, 174-8168, 174-  
9842, 378-2111 Интернет:  
<http://www.nelk.ru> E-mail: [nelk@aha.ru](mailto:nelk@aha.ru)

## Универсальная программа обнаружения средств негласного съема информации ФИЛИН



Это универсальная базовая программа обнаружения средств негласного съема информации передачей полезного сигнала на радиочастоте (включая TV передатчики). Возможно управление сканирующими приемниками Winradio, AR-3000A, AR-8000, AR 8200, AR-5000, AR-2700, IC-R10, IC-R7000, IC-7100, IC-R8500, IC-R9000 и IC-PCR1000, анализаторами спектра фирмы Hewlett Packard и другим оборудованием.

До шести (!) одновременно используемых прогрессивных алгоритмов обнаружения. Высокая вероятность обнаружения при низком уровне ложной тревоги. Возможность автоматической классификации цифровых каналов передачи данных, что существенно облегчает обнаружение цифровых радиозакладок. Полностью автоматизирована. С возможностью детального анализа принимаемых сигналов по их спектральным составляющим, осциллограммам, корреляционным функциям и др. Операционная система не ниже Windows 95.



НАУЧНО-ПРОИЗВОДСТВЕННЫЙ ЦЕНТР "НЕПК"  
109377, Россия, Москва, 1-ая  
Иовонюзьминская улица, дом 8/2 тел.:  
+7-1095) 174-9264, 174-9168, 174-9842,  
378-2111 Интернет: <http://wnMw.nelk.ru> E-  
mail: [nelk@aha.ru](mailto:nelk@aha.ru)



## Универсальный пакет программ радиомониторинга ПАТРУЛЬ



Это пакет программ, обеспечивающий сбор, хранение и анализ результатов радиоконтроля.

Патруль состоит из двух программных модулей:

- управления радиоприемными устройствами (РПУ) и сбора данных Патруль,
- обработки данных радиоконтроля - Контроль.

Модуль управления РПУ и сбора данных обеспечивает управление одним или двумя РПУ, а также получение данных о географическом местоположении в системе GPS и отображения на фоне карт местности в формате Map Info.

Позволяет решать различные задачи радиоконтроля:

- контроль диапазонов или групп частот,
- идентификация обнаруженных сигналов,
- измерение параметров излучения,
- выявление отклонений параметров сигналов от установленных норм,
- оценка занятости частотных диапазонов и интенсивности использования фиксированных частот,
- запись, хранение и обработка фонограмм.

Программа имеет эффективные средства анализа низкочастотного сигнала: осциллограф, анализатор спектра, спектрограмма.

Результаты радиоконтроля автоматически сохраняются в базах данных и в дальнейшем могут быть использованы для анализа.

Модуль обработки данных предназначен для обработки результатов радиоконтроля, полученных в результате работы программы Патруль. Позволяет проводить анализ работы радиоэлектронных средств на определенной частоте или в диапазоне частот. Имеется возможность проведения выборок по времени работы радиосредств, географическому положению, характеристикам передатчика.

Обеспечивает: статистическую обработку результатов контроля; отображение местоположения РЭС на карте; редактирование баз данных результатов контроля, частотных присвоений; построение следующих графических диаграмм: время/занятость канала, время/параметр излучения, время/отклонение параметра излучения.



НАУЧНО-ПРОИЗВОДСТВЕННЫЙ ЦЕНТР "НЕЛК"  
109377, Россия, Москва, 1-ая  
Новокузьминская улица, дом 8/2 теп.:  
+7-(095) 174-9264, 174-9168, 174-  
9842, 378-2111 Интернет:  
<http://www.nelk.ru> E-mail: [nelk@aha.ru](mailto:nelk@aha.ru)

# 1

## Персональный телефонный секретарь - цифровой магнитофон WINMAG

Позволяет реализовать на мультимедийном компьютере высококачественную систему регистрации, хранения обработки телефонных разговоров и любых других фонограмм с широкими сервисными возможностями.

### Особенности:

- Не требует никакого дополнительного оборудования - аппаратных приставок и т.д.
- Может вести запись независимо с двух телефонных линий одновременно!
- Минимальные требования к компьютеру Pentium 166/16 Мб/звуковая карта.
- Регулируемый режим активации голосом (акусто-старт, акусто-стоп), возможность «сжатия» пауз.
- Сигнализация основных событий.
- Редактирование ранее записанных фонограмм.
- Возможность комментирования фонограмм и ведения архивов.

*Оптимальное соотношение цена / возможности//!*

**Может использоваться для:** запись телефонных разговоров с регистрацией времени начала разговора и его длительности; запись через выносной микрофон переговоров, ведущихся в помещении (до двух помещений одновременно); оцифровка аудиоинформации с любых носителей (перезапись с аудиокассет, аудио компакт-дисков и т.п.); хранение, сортировка и комментирование записанной аудиоинформации; редактирование записей фонограмм работа с буфером обмена, базовые операции редактирования, склейка файлов; прослушивание записанных фонограмм или их фрагментов.



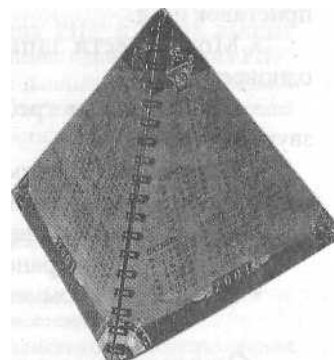
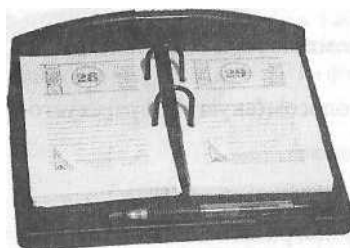
НАУЧНО-ПРОИЗВОДСТВЕННЫЙ ЦЕНТР "НЕЛК"  
109377, Россия, Москва, 1-ая  
Новокузьминская улица, дом 8/2 тел.:  
+7-(095) (74-9264, 174-9168, 174-  
9842,378-2111 Интернет:  
<http://www.nelk.ru> E-mail: [nelk@aha.ru](mailto:nelk@aha.ru)

---

## Индикатор радиоволн «Пирамида»

### Назначение:

- Выявление скрыто носимых радио микрофонов у Ваших посетителей.
- Выявление мощных (СВЧ) электромагнитных полей, которые создают подавители микрофонов и радио микрофонов.
- Для обнаружения вредных излучений микроволновых печей.
- Для обнаружения радио закладок, телефонных, акустических и телевизионных.
- Виды камуфляжа: сменный, перекидной календарь, сувенир в виде коллекционного вина.



### Основные технические характеристики:

Диапазон контролируемых частот

Питание (батарея типа «КРОНА»)

Индикация постоянная световая и  
отключаемая звуковая

Ток потребления в ждущем режиме  
в режиме индикации

Время непрерывной работы не менее

Дальность обнаружения носимых радио микрофонов

**60-3000 МГц**

9В

**(3 тел. звонка)**

**0,55 мА**

5мА.

**5 суток**

4-5 м.