В.С. Солодкий
В.А. Тимофеев

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ С ОГРАНИЧЕННЫМ ДОСТУПОМ

Харьков 2013

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ

ХАРЬКОВСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ
РАДИОЭЛЕКТРОНИКИ

В.С. Солодкий
В.А. Тимофеев

Технические средства защиты информации с ограниченным доступом

Харьков 2013

УДК 338 (447)
ББК – У9

Рекомендовано к печати Ученым советом Харьковского национального университета радиоэлектроники (протокол №16 от 30 ноября 2012 г.)

Рецензенты: Т.В. Момот – доктор экономических наук, профессор кафедры управления финансово-экономической безопасностью, учета и аудита Харьковской национальной академии городского хозяйства;

И.В. Чумаченко – доктор технических наук, профессор, декан факультета менеджмента Национального аэрокосмического университета «ХАИ»

Солодкий В.С., Тимофеев В.А.
Технические средства защиты информации с ограниченным доступом [Текст]: Монография.- Харьков: ХНУРЭ, 2013.- 228 с.

В предлагаемой книге сделана попытка систематизировать разрозненные сведения по проблеме защиты информации от различных видов и средств технической разведки, изложены основы методологии обеспечения защиты информационных систем, в том числе каналов передачи данных. Определена сущность задач обеспечения информационной безопасности телекоммуникационных систем, раскрыты основы правового регулирования защиты информации в этих системах.

Книга предусмотрена для студентов специальности 8.18010014 «Управление финансово-экономической безопасностью» для изучения дисциплин «Комплексное обеспечение финансово-экономической безопасности», «Правовое обеспечение безопасности субъектов хозяйственной деятельности в Украине», «Организация защиты информации на предприятии», а также для практических работников в области защиты информации с ограниченным доступом.

ISBN 978-966-7735-62-3

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В общем комплексе мероприятий по ведению разведки важное место отводится технической разведке, которая в настоящее время считается основным средством получения разведывательной информации.

Считается, что на долю технической разведки приходится более 50% всей добываемой информации. Поэтому проблема защиты от технической разведки приобретает особую актуальность.

Защита от технических средств защиты информации (ТСР) является неотъемлемой и составной частью научной и производственной деятельности предприятий, учреждений и организаций всех форм собственности.

Необходимо отметить также, что на современном этапе широкое распространение находит экономический и промышленный шпионаж, который не связан непосредственно с межгосударственными, политическими и военными противоречиями.

Главной причиной возникновения промышленного (экономического) шпионажа является конкуренция между фирмами, компаниями и предприятиями. Промышленный шпионаж охватывает сегодня все сферы рыночной экономики и в условиях ожесточенной конкурентной борьбы его масштабы резко возрастают.

При ведении промышленного шпионажа пользуются теми же техническими средствами и способами. Поэтому материал предлагаемой книги, безусловно, является полезным для широкого круга лиц, в обязанности которых входят вопросы обеспечения безопасности информации.

Неотъемлемой частью защиты скрываемых объектов и информации от разведки является технический контроль, который предназначен для оценки эффективности и надежности принимаемых мер защиты. Без качественного технического контроля невозможно реализовать надежное закрытие каналов утечки информации.

Техническая защита информации в системах обработки и передачи данных должна осуществляться в строгом соответствии с нормативными документами. Поэтому в работе должное внимание уделено вопросам правового обеспечения комплексной системы технических средств защиты информации, а также передачи информации в телекоммуникационных системах.

1 ТЕХНИЧЕСКИЕ СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

1.1 Виды, источники и носители защищаемой информации

Значение информации в жизни любого цивилизованного общества непрерывно возрастает. С незапамятных времен сведения, имеющие важное военно-стратегическое значение для государства, тщательно скрывались и защищались. В настоящее время информация, относящаяся к технологии производства и сбыта продукции, стала рыночным товаром, имеющим большой спрос как на внутреннем, так и на внешнем рынках. Информационные технологии постоянно совершенствуются в направлении их автоматизации и способов защиты информации.

Развитие новых информационных технологий сопровождаются такими негативными явлениями, как промышленный шпионаж, компьютерные преступления и несанкционированный доступ (НСД) к секретной, служебной и конфиденциальной информации. Поэтому защита информации является важнейшей государственной задачей в любой стране.

Защита информации должна обеспечивать предотвращение ущерба в результате утери (хищения, утраты, искажения, подделки) информации в любом ее виде. Организация мер защиты информации должна проводиться в полном соответствии с действующими законами и нормативными документами по безопасности информации, интересами пользователей информации. Чтобы гарантировать высокую степень защиты информации, необходимо постоянно решать сложные научно-технические задачи разработки и совершенствования средств ее защиты.

Большинство современных предприятий независимо от вида деятельности и форм собственности не может успешно вести хозяйственную и иную деятельность без обеспечения системы защиты своей информации, включающей организационно-нормативные меры и технические средства контроля безопасности информации при ее обработке, хранении и передаче в автоматизированных системах (АС).

Собственниками (или владельцами) защищаемой информации могут быть органы государственной власти и образуемые ими структуры (государственная тайна, служебная тайна, в определенных случаях коммерческая и банковская тайны); юридические лица (коммерческая, банковская, служебная, адвокатская, врачебная, аудиторская тайны и т.п.); общественные организации (партийная тайна, не исключена также государственная и коммерческая тайна); граждане государства (физические лица) – в отношении персональных данных, нотариальной, адвокатской, врачебной.

Защищаемая информация обладает следующими свойствами [71]:

- уровень доступа к ней, ограничения на порядок распространения и использования может устанавливать только владелец или наделенные таким правом определенные лица;

- чем ценнее для собственника информация, тем тщательнее она защищается и тем меньшее число лиц имеет доступ к этой информации.

Информация по форме представления, способам кодирования и хранения может быть графической, звуковой, текстовой, цифровой (компьютерной), видеоинформацией и т.п.

Наиболее важными свойствами информации являются, прежде всего, ее достоверность, полнота, объективность, своевременность, важность.

Для хранения как секретной, так и несекретной информации применяются одни и те же носители. В общем случае носители секретной и конфиденциальной информации охраняются ее собственником.

Носители защищаемой информации классифицируются следующим образом [71]:

- документы;
- изделия (предметы);
- вещества и материалы;
- электромагнитные, тепловые, радиационные и другие излучения;
- гидроакустические, сейсмические и другие физические поля, представляющие особые виды материи;
- сам объект с его видовыми характеристиками и т.п.

В качестве носителя защищаемой информации может быть также человек.

Формы представления информации зависят от его характера и физических носителей, на которых она представлена. Основными формами информации, подлежащими защите, являются:

- документальные;
- акустические;
- телекоммуникационные;
- видовые.

Документ – представленная на материальном носителе информация с идентификатором, позволяющим установить характер документа и его собственника. Информация, записанная на носителе, может быть графической и текстовой. На документе-носителе защищаемой информации указывается степень конфиденциальности информации в зависимости от ее важности.

Источниками речевой информации являются разговоры в помещениях и системы звуковоспроизведения. Речевая информация распространяется в газовой, твердотельной и гидравлической средах. Носителем речевой информации являются акустические колебания частиц в виде звуковых волн различной длины в упругих средах. Слышимый речевой сигнал находится в диапазоне частот 200 Гц – 6 кГц.

Изделия (предметы) как носители защищаемой информации могут представлять собой засекреченные образцы военной техники, опытные образцы вновь разрабатываемых высокотехнологичных изделий и систем, определяющих уровень научно-технического развития промышленности страны.

Материалы и вещества, применяемые в производстве и эксплуатации новых образцов техники и в военных изделиях. Отметим особо, что иностранные разведки могут получать информацию о материалах и веществах наиболее

доступными способами – по отходам производства режимных предприятий, по составу воздушной среды и водных осадков в непосредственной близости от предприятия.

Электромагнитные излучения различной частоты могут содержать информативные сигналы от защищаемого объекта при его функционировании. Источником электромагнитного излучения в большинстве случаев являются кабельные и проводные линии каналов передачи информации. Опасными являются также вспомогательные средства и системы, представляющие собой сосредоточенные и распределенные случайные антенны.

Носителем видовой информации объекта является сам объект, а также его фото- и видеоизображения на материальных носителях информации.

С развитием информационного общества все большее значение приобретают проблемы, связанные с защитой информации с ограниченным доступом. Информация как категория, имеющая стоимость, защищается ее собственником от лиц и организаций, пытающимся ею завладеть. Общая тенденция такова, что чем выше уровень секретности информации, тем выше и уровень ее защиты, тем больше средств затрачивается на ее защиту.

1.2 Задачи и объекты систем защиты информации

Защита информации представляет собой комплекс целенаправленных мероприятий ее собственников по предотвращению утечки, искажения, уничтожения и модификации защищаемых сведений.

Под системой защиты информации можно понимать государственную систему защиты информации и систему защиты информации на конкретных объектах [71].

Государственная система защиты информации включает в себя:

- систему государственных нормативных актов, стандартов, руководящих документов и требований;
- разработку концепций, требований, нормативно-технических документов и научно-методических рекомендаций по защите информации;
- порядок организации, функционирования и контроля за выполнением мер, направленных на защиту информации, которая принадлежит к государственным информационным ресурсам, а также рекомендаций по защите информации, находящейся в собственности физических и юридических лиц;
- организацию испытаний и сертификации средств защиты информации;
- создание ведомственных и отраслевых координационных структур для защиты информации;
- осуществление контроля за выполнением работ по организации защиты информации;
- определение порядка доступа юридических и физических лиц иностранных государств к информации, которая принадлежит к государственным информационным ресурсам, или к информации физических и юридических лиц,

относительно распространения и использования которой государством установлены ограничения.

Цели защиты информации от технических средств разведки на конкретных объектах информатизации определяются конкретным перечнем потенциальных угроз. В общем случае цели защиты информации можно сформулировать как [71]:

- предотвращение утечки, хищения, утраты, искажения, подделки информации;
- предотвращение угроз безопасности личности, общества, государства;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;
- предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;
- сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;
- обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Эффективность защиты информации определяется ее своевременностью, активностью, непрерывностью и комплексностью. Очень важно проводить защитные мероприятия комплексно, то есть обеспечивать нейтрализацию всех опасных каналов утечки информации. Необходимо помнить, что даже один-единственный не закрытый канал утечки может свести на нет эффективность системы защиты.

Основными объектами защиты информации являются [76]:

- информационные ресурсы, содержащие сведения, связанные с государственной тайной и конфиденциальной информацией;
- средства и информационные системы (средства вычислительной техники, сети и системы), программные средства (операционные системы, системы управления базами данных, прикладное программное обеспечение), автоматизированные системы управления, системы связи и передачи данных, технические средства приёма, передачи и обработки информации ограниченного доступа (звукозапись, звукоусиление, звуковоспроизведение, переговорные и телевизионные устройства, средства изготовления, тиражирование документов и другие технические средства обработки графической, смысловой и буквенно-цифровой информации), т.е. системы и средства, непосредственно обрабатывающие конфиденциальную информацию и информацию, относящуюся к категории государственной тайны. Эти средства и системы часто называют техническими средствами приёма, обработки и хранения информации (ТСПИ);
- технические средства и системы, не входящие в состав ТСПИ, но территориально находящиеся в помещениях обработки секретной и конфиденциальной информации. Такие технические средства и системы

называются вспомогательными техническими средствами и системами (ВТСС). К ним относятся: технические средства телефонной, громкоговорящей связи, системы пожарной и охранной сигнализации, радиотрансляции, часофикации, средства и системы передачи данных в системе радиосвязи, контрольно-измерительная аппаратура, электробытовые приборы и т.д., а также сами помещения, предназначенные для обработки информации ограниченного распространения;

- ТСПИ можно рассматривать как систему, включающую стационарное оборудование, периферийные устройства, соединительные линии, распределительные и коммуникационные устройства, системы электропитания, системы заземления.

Технические средства, предназначенные для обработки конфиденциальной информации, включая помещения, в которых они размещаются, представляют *объект ТСПИ*.

1.3 Технические каналы утечки информации. Структура, классификация и основные характеристики

Наибольший интерес с точки зрения образования каналов утечки информации представляют ТСПИ и ВТСС, имеющие выход за пределы *контролируемой зоны* (КЗ), т.е. зоны с пропускной системой. Кроме соединительных линий ТСПИ и ВТСС за пределы контролируемой зоны могут иметь выход проходящие через помещения посторонние проводники, не связанные с ТСПИ и ВТСС (рис. 1.1) [71].

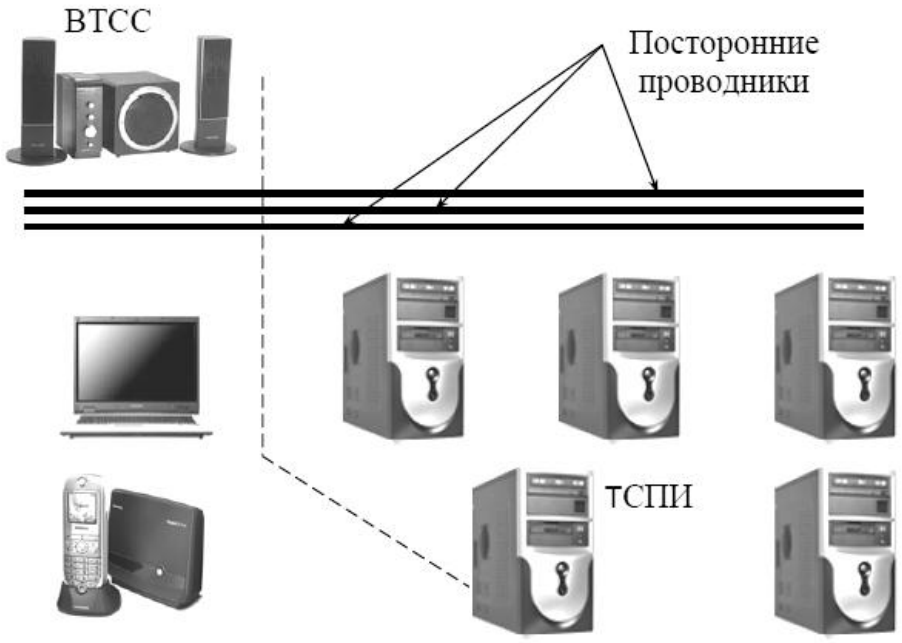


Рисунок 1.1 - Источники образования возможных каналов утечки информации

Зона с возможностью перехвата разведывательным оборудованием побочных электромагнитных излучений, содержащих конфиденциальную информацию, называется *опасной зоной*. Пространство вокруг ТСПИ, в котором на случайных антеннах наводится информационный сигнал выше допустимого уровня, называется *опасной зоной* 1 [71].

Случайными антеннами могут быть цепи ВТСС или посторонние проводники, воспринимающие побочные электромагнитные излучения от средств ТСПИ. Случайные антенны бывают сосредоточенными и распределёнными. Сосредоточенная случайная антенна представляет собой техническое средство с сосредоточенными параметрами (телефонный аппарат, громкоговоритель радиотрансляционной сети и т.д.). Распределённые случайные антенны образуют проводники с распределёнными параметрами: кабели, соединительные провода, металлические трубы.

Информационные сигналы могут быть электрическими, электромагнитными, акустическими и т.д. Они имеют в большинстве случаев колебательный характер, а информационными параметрами являются амплитуда, фаза, частота, длительность.

Под техническим каналом утечки информации (ТКУИ) понимают совокупность объекта разведки, технического средства разведки (ТСР) и физической среды, в которой распространяется информационный сигнал (рис. 1.2). В сущности, под ТКУИ понимают способ получения с помощью ТСР разведывательной информации об объекте [71].

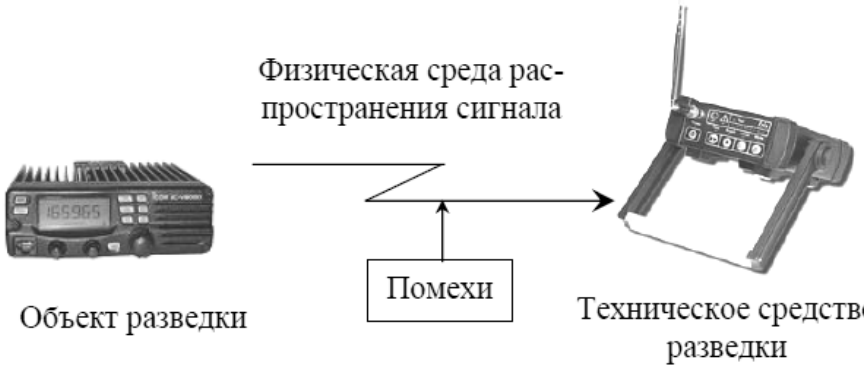


Рисунок 1.2 - Технический канал утечки информации (ТКУИ)

В зависимости от физической природы сигналы распространяются в определенных физических средах. Средой распространения могут быть газовые (воздушные), жидкостные (водные) и твердые среды. К таким средам относятся воздушное пространство, конструкции зданий, соединительные линии и токопроводящие элементы, грунт и т.п.

Противодействие промышленному и экономическому шпионажу является непрерывным и адекватным новым типам угроз процессом развития методов, средств и способов защиты информации.

Классификация каналов утечки информации представлена на рис. 1.3.

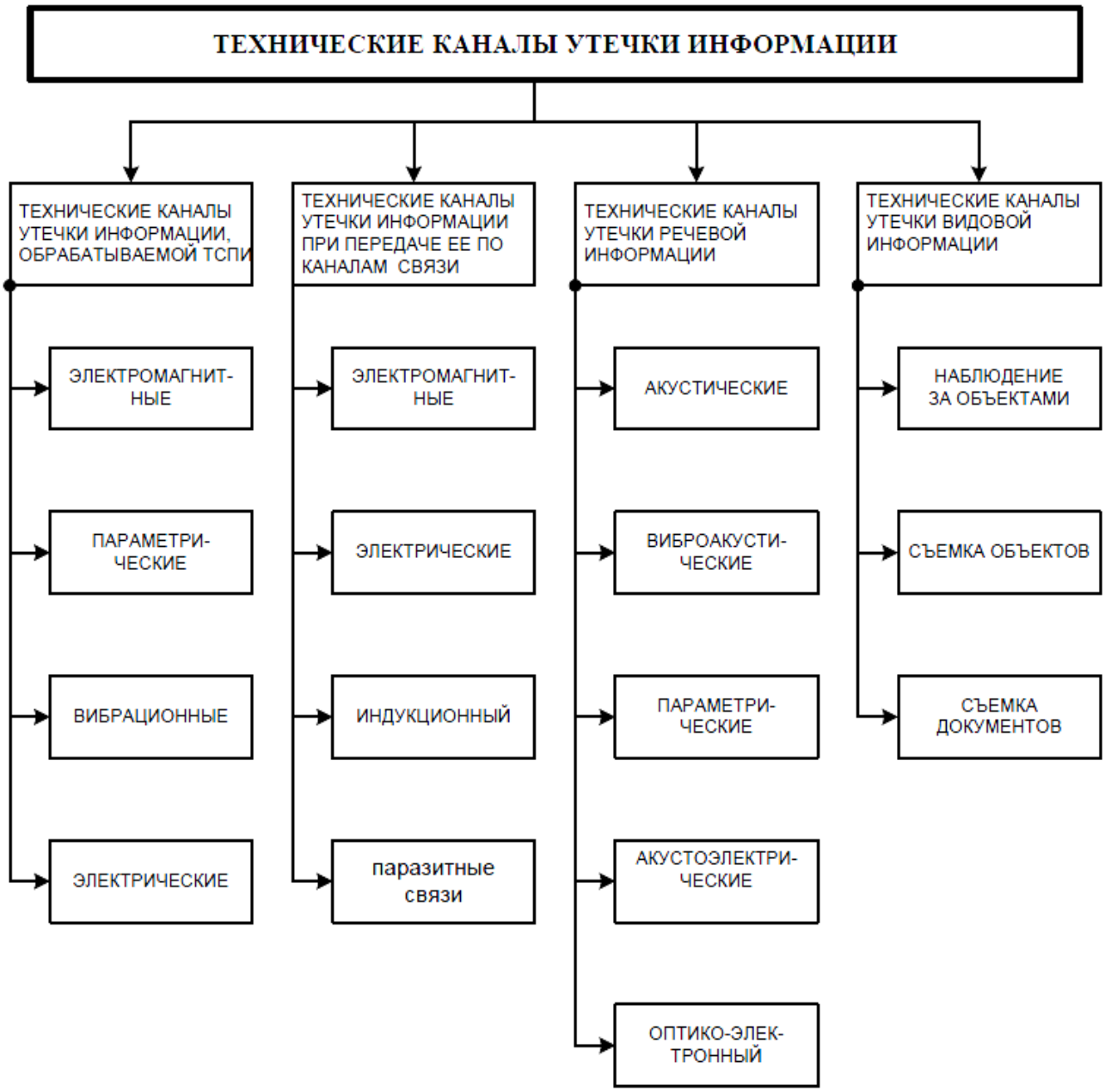


Рисунок 1.3 - Технические каналы утечки информации

Особенности технических каналов утечки информации определяются физической природой информационных сигналов и характеристиками среды распространения сигналов утекаемой информации. Ниже приведены некоторые особенности технических каналов утечки информации [71].

Технические каналы утечки информации, обрабатываемой ТСПИ

1) Электромагнитные:

- электромагнитные излучения элементов ТСПИ;
- электромагнитные излучения на частотах работы ВЧ-генераторов ТСПИ;
- излучения на частотах самовозбуждения усилителей низкой частоты.

2) Электрические:

- наводки электромагнитных излучений элементов ТСПИ на посторонние проводники;

- просачивание информационных сигналов в линии электропитания;
- просачивание информационных сигналов в цепи заземления;
- съем информации с использованием закладных устройств.

3) Параметрические:

- перехват информации путем «высокочастотного облучения» ТСПИ.

4) Вибрационные:

- соответствие между распечатываемым символом и его акустическим образом.

Технические каналы утечки информации при передаче ее по каналам связи

1) Электромагнитные каналы:

- электромагнитные излучения передатчиков связи, модулированные информационным сигналом (прослушивание радиотелефонов, сотовых телефонов, радиорелейных линий связи).

2) Электрические каналы:

- подключение к линиям связи.

3) Индукционный канал:

- эффект возникновения вокруг высокочастотного кабеля электромагнитного поля при прохождении информационных сигналов.

4) Паразитные связи:

- паразитные емкостные, индуктивные и резистивные связи и наводки близко расположенных друг от друга линий передачи информации.

Технические каналы утечки речевой информации

1) Акустические каналы:

- среда распространения – воздух.

2) Виброакустические каналы:

- среда распространения – ограждающие строительные конструкции.

3) Параметрические каналы:

- результат воздействия акустического поля на элементы схем, что приводит к модуляции высокочастотного сигнала информационным.

4) Акустоэлектрические каналы:

- преобразование акустических сигналов в электрические.

5) Оптико-электронный (лазерный) канал:

- облучение лазерным лучом вибрирующих поверхностей.

Технические каналы утечки видовой информации

1) Наблюдение за объектами.

Для наблюдения днем применяются оптические приборы и телевизионные камеры. Для наблюдения ночью – приборы ночного видения, тепловизоры, телевизионные камеры.

2) Съемка объектов.

Для съемки объектов используются телевизионные и фотографические средства. Для съемки объектов днем с близкого расстояния применяются портативные камуфлированные фотоаппараты и телекамеры, совмещенные с устройствами видеозаписи.

3) Съемка документов.

Съемка документов осуществляется с использованием портативных фотоаппаратов.

1.3.1 Технические каналы утечки информации, обрабатываемой ТСПИ

Электромагнитные каналы утечки информации ТСПИ

Основным каналом утечки информации при ее обработке ТСПИ является электромагнитный канал, обусловленный побочными информативными электромагнитными излучениями основных технических средств обработки информации. К *электромагнитным* относятся каналы утечки информации, возникающие за счет различного вида побочных электромагнитных излучений ТСПИ. Побочные электромагнитные излучения (ПЭМИ) – это паразитные электромагнитные излучения радиодиапазона, создаваемые в окружающем пространстве устройствами, специальным образом для этого не предназначенными.

К побочным электромагнитным излучениям ТСПИ относятся [71]:

- излучения элементов ТСПИ;
- излучения на частотах работы высокочастотных (ВЧ) генераторов ТСПИ;
- излучения на частотах самовозбуждения усилителей низкой частоты (УНЧ) ТСПИ.

Электромагнитные излучения элементов ТСПИ. В ТСПИ, в частности и в линиях связи, входящих в их состав, носителем информации является электрический ток, характеристики которого (сила тока, напряжение, частота и фаза) изменяются по закону информационного сигнала. При прохождении электрического тока по проводникам ТСПИ вокруг них в окружающем пространстве возникает электрическое и магнитное поле. По этой причине элементы ТСПИ можно рассматривать как излучатели электромагнитного поля, составляющие которого модулированы также по закону изменения информационного сигнала.

Высокочастотные электромагнитные излучения передатчиков средств связи, модулированные информационным сигналом, могут перехватываться портативными средствами радиоразведки и при необходимости передаваться в центр обработки для их раскодирования.

Данный канал перехвата информации наиболее широко используется для прослушивания телефонных разговоров, ведущихся по радиотелефонам, сотовым телефонам или по радиорелейным и спутниковым линиям связи.

Электромагнитные излучения персональных компьютеров. Согласно оценочным данным по каналу ПЭМИН (побочных электромагнитных излучений и наводок) может быть перехвачено не более 1–2 процентов данных, обрабатываемых на персональных компьютерах и других технических средствах передачи информации (ТСПИ). На первый взгляд может показаться, что этот канал менее опасен по сравнению, например, с акустическим, по которому из помещения может быть перехвачена речевая информации в полном объеме. Но

необходимо помнить, что в настоящее время наиболее важная информация, содержащая государственную тайну или технологические секреты, обрабатывается на персональных компьютерах. Специфика канала ПЭМИН такова, что те самые два процента информации, уязвимые для технических средств перехвата – это данные, вводимые с клавиатуры компьютера или отображаемые на мониторе [71].

Компьютеры порождают электромагнитные излучения, которые не только создают помехи для радиоприема, но также создают технические каналы утечки информации. Соединительные кабели (линии связи), обладающие индуктивностью и емкостью, образуют резонансные контуры, излучающие высокочастотные электромагнитные волны, модулированными сигналами данных.

Аналогичная ситуация имеет место и при взаимном обмене сигналами между параллельно проложенными кабелями. Исследователями продемонстрировано восстановление сетевых данных через телефонную линию, причем телефонный кабель проходил рядом с кабелем компьютерной сети всего на протяжении двух метров. Еще одна опасность исходит от «активных» атак (высокочастотное навязывание): злоумышленник, знающий резонансную частоту, например, кабеля клавиатуры персонального компьютера, может облучать его на этой частоте, а затем регистрировать коды нажатия клавиш в ретранслируемом резонансном сигнале благодаря вызванным ими изменениям импеданса [71].

Для ПК высокочастотные излучения находятся в диапазоне до 1 ГГц с максимумом в полосе 50–300 МГц. Широкий спектр обусловлен наличием как основной, так и высших гармоник последовательностей коротких прямоугольных информационных импульсов. К появлению дополнительных составляющих в побочном электромагнитном излучении приводит также применение в вычислительных средствах высокочастотной коммутации.

Говорить о какой-либо диаграмме направленности электромагнитных излучений ПК не имеет смысла, так как расположение его составных частей имеет много комбинаций. ПК имеет линейную поляризацию. Она определяется расположением соединительных кабелей, являющихся основными источниками излучений в ПК с металлическим кожухом на системном блоке.

Уровни побочных электромагнитных излучений ВТ регламентированы по условиям электромагнитной совместимости целым рядом зарубежных и отечественных стандартов. Так, например, согласно публикации «№ 22 CISPR (специальный международный комитет по радиопомехам) для диапазона 230–1000 МГц уровень напряженности электромагнитного поля, излучаемого оборудованием ВТ, на расстоянии 10 м не должен превышать 37 дБ. Однако излучения такого уровня могут быть перехвачены на значительных расстояниях. Следовательно, соответствие электромагнитных излучений средств ВТ нормам на электромагнитную совместимость не обеспечивает сохранение конфиденциальности обрабатываемой в них информации [71].

Электромагнитные излучения на частотах работы ВЧ генераторов ТСПИ и ВТСС. В состав ТСПИ и ВТСС могут входить различного рода высокочастотные генераторы как-то: задающие генераторы, генераторы тактовой частоты,

генераторы стирания и подмагничивания магнитофонов, гетеродины радиоприемных устройств, генераторы измерительных приборов и т.д. [71].

При внешних воздействиях информационного сигнала (например, электромагнитных полей) на элементах ВЧ генераторов индуктируются электрические сигналы. Приемными антеннами для магнитного поля могут служить катушки индуктивности колебательных контуров, сглаживающие дроссели в цепях электропитания и т.д. Приемниками электрического поля являются провода высокочастотных цепей и другие элементы. Индуктированные электрические сигналы могут вызвать модуляцию собственных ВЧ колебаний генераторов и излучение их в окружающее пространство.

Электромагнитные излучения на частотах самовозбуждения УНЧ ТСПИ. Самовозбуждение УНЧ ТСПИ (например, усилителей систем звукоусиления и звукового сопровождения, магнитофонов, систем громкоговорящей связи т.п.) возможно за счет преобразований отрицательных обратных связей (индуктивных или емкостных) в паразитные положительные в результате фазового сдвига сигнала обратной связи на определенных частотах, что приводит к переводу усилителя из режима усиления в режим автогенерации сигналов. Частота самовозбуждения находится в пределах рабочих частот элементов УНЧ (например, полупроводниковых приборов, электровакуумных ламп и т.п.), переходящих в нелинейный режим работы при перегрузке за счет действия положительной обратной связи. Сигнал на частотах самовозбуждения, как правило, оказывается промодулированным информационным сигналом. Перехват побочных электромагнитных излучений ТСПИ осуществляется средствами радио-, радиотехнической разведки, размещенными за пределами контролируемой зоны [71].

Зона, в которой возможен перехват побочных электромагнитных излучений с помощью разведывательного приемника с последующей расшифровкой содержащейся в них информации (т.е. зона, в пределах которой отношение «информационный сигнал/помеха» превышает допустимое нормированное значение), называется опасной *зоной 2.*

Электрические каналы утечки информации, обрабатываемой ТСПИ

Электрические каналы утечки информации образуются за счет [71]:

- наводок электромагнитных излучений ТСПИ на соединительные линии ВТСС и посторонние проводники, выходящие за пределы контролируемой зоны;
- просачивания информационных сигналов в цепи электропитания ТСПИ;
- просачивания информационных сигналов в цепи заземления ТСПИ.

Наводки возникают при излучении элементами ТСПИ (в том числе и их соединительными линиями) информационных сигналов, а также при наличии гальванической связи соединительных линий ТСПИ и посторонних проводников или линий ВТСС. Уровень наводимых сигналов в значительной степени зависит от мощности излучаемых сигналов, расстояния до проводников, а также длины соединительных линий ТСПИ и посторонних проводников [71].

Пространство вокруг ТСПИ, в пределах которого на случайных антеннах наводится информационный сигнал выше нормированного уровня, называется (опасной) *зоной 1.*

Случайными антеннами могут быть цепи ВТСС или посторонние проводники, способные принимать побочные электромагнитные излучения.

Случайные антенны могут быть сосредоточенными и распределенными. *Сосредоточенная случайная антенна* представляет собой техническое средство небольшого объема, например телефонный аппарат, громкоговоритель радиотрансляционной сети, реле и т.д. К *распределенным случайным антеннам* относятся случайные антенны с распределенными параметрами (длинные линии): кабели, провода, металлические трубы и другие токопроводящие устройства.

Просачивание информационных сигналов в цепи электропитания. Просачивание возможно при наличии взаимоиндуктивной связи между выходным трансформатором усилителя (например, УНЧ) и трансформатором выпрямительного устройства. Кроме того, токи усиливаемых информационных сигналов замыкаются через источник электропитания, создавая на его внутреннем сопротивлении падение напряжения, которое при недостаточном затухании в фильтре выпрямительного устройства может быть обнаружено в линии электропитания. Информационный сигнал может проникнуть в цепи электропитания также в результате того, что среднее значение потребляемого тока в оконечных каскадах усилителей в большей или меньшей степени зависит от амплитуды информационного сигнала, что создает неравномерную нагрузку на выпрямитель и приводит к изменению потребляемого тока по закону изменения информационного сигнала.

Наводки на вторичные источники питания (ВИП), можно разделить на три вида: наводки в виде переменного напряжения с частотой питающей сети или ее гармоник, высокочастотные наводки, появляющиеся вследствие антенного эффекта проводов питающей сети, наводки, возникающие внутри блока вследствие появления паразитных связей через общие провода питания различных элементов [71].

Основными причинами появления помехи с частотой питающей сети или ее гармоник являются недостаточное сглаживание пульсаций в ВИП, паразитные связи элементов с первичными цепями ВИП, неэквипотенциальность точек заземления, наличие общих проводов питания, по которым возможна гальваническая связь. Из всех причин только первая не является следствием паразитных процессов. Величина наводки зависит не только от вида паразитной связи, но и от схемы подключения двухфазных ВИП к трехфазной промышленной сети.

Просачивание информационных сигналов в цепи заземления. Кроме заземляющих проводников, служащих для непосредственного соединения ТСПИ с контуром заземления, гальваническую связь с землей могут иметь различные проводники, выходящие за пределы контролируемой зоны. К ним относятся нулевой провод сети электропитания, экраны (металлические оболочки) соединительных кабелей, металлические трубы систем отопления и водоснабжения, металлическая арматура железобетонных конструкций и т.д. Все эти проводники совместно с заземляющим устройством образуют разветвленную систему заземления, в которой могут наводиться информационные сигналы.

Кроме того, в грунте вокруг заземляющего устройства возникает электромагнитное поле, которое также является источником информации [71].

Перехват информационных сигналов по электрическим каналам утечки возможен путем непосредственного подключения к соединительным линиям ВТСС и посторонним проводникам специальных устройств съема информации. Для перехвата электромагнитных сигналов используются специальные средства радио- и радиотехнической разведки.

Съем информации по электрическим каналам утечки информации. Для съема информации, обрабатываемой в ТСПИ, применяют главным образом электронные устройства перехвата информации – *закладные устройства.* Электронные устройства перехвата информации, устанавливаемые в ТСПИ, иногда называют *аппаратными закладками.* Они представляют собой мини-передатчики, излучение которых модулируется информационным сигналом. Закладки устанавливаются в ТСПИ как иностранного так отечественного производства.

Перехваченная с помощью закладных устройств информация или непосредственно передается по радиоканалу, или сначала накапливается на специальном запоминающем устройстве, а уже затем по сигналу извне передается на запросивший ее объект.

Электрический канал перехвата информации, передаваемой по кабельным линиям связи, предполагает контактное подключение аппаратуры разведки к кабельным линиям связи.

Самый простой способ – это непосредственное параллельное подключение к линии связи. Но данный факт легко обнаруживается, так как приводит к изменению характеристик линии связи за счет падения напряжения. Поэтому средства разведки к линии связи подключаются или через согласующее устройство, несколько снижающее падение напряжения, или через специальные устройства компенсации падения напряжения. В последнем случае аппаратура разведки и устройство компенсации падения напряжения включаются в линию связи последовательно, что существенно затрудняет обнаружение факта несанкционированного подключения к ней [71].

Контактный способ используется в основном для снятия информации с коаксиальных и низкочастотных кабелей связи. Для кабелей, внутри которых поддерживается повышенное давление воздуха, применяются устройства, исключающие его снижение, в результате чего предотвращается срабатывание специальной сигнализации.

Электрический канал наиболее часто используется для перехвата телефонных разговоров. При этом перехватываемая информация может непосредственно записываться на диктофон или передаваться по радиоканалу в пункт приема для ее записи и анализа. Устройства, подключаемые к телефонным линиям связи и комплексированные с устройствами передачи информации по радиоканалу, часто называют *телефонными закладками* [71].

В случае использования сигнальных устройств контроля целостности линии связи, ее активного и реактивного сопротивления факт контактного подключения к ней аппаратуры разведки будет обнаружен. Поэтому спецслужбы наиболее

часто используют индуктивный канал перехвата информации, не требующий контактного подключения к каналам связи. В данном канале используется эффект возникновения вокруг кабеля связи электромагнитного поля при прохождении по нему информационных электрических сигналов, которые перехватываются специальными индукционными датчиками. Индукционные датчики используются в основном для съема информации с симметричных высокочастотных кабелей. Сигналы с датчиков усиливаются, осуществляется частотное разделение каналов, и информация, передаваемая по отдельным каналам, записывается на магнитофон или высокочастотный сигнал записывается на специальный магнитофон.

Современные индукционные датчики способны снимать информацию с кабелей, защищенных не только изоляцией, но и двойной броней из стальной ленты и стальной проволоки, плотно обвивающих кабель.

Для бесконтактного съема информации с незащищенных телефонных линий связи могут использоваться специальные низкочастотные усилители, снабженные магнитными антеннами.

Некоторые средства бесконтактного съема информации, передаваемой по каналам связи, могут комплексироваться с радиопередатчиками для ретрансляции в центр ее обработки.

Исходя из выше перечисленных особенностей ТСПИ и ВТСС, а также возможностей современных технических разведок можно заключить, что всегда существует потенциальная опасность возникновения технического канала утечки информации. И эта проблема должна решаться за счет совершенствования применяемого оборудования (ТСПИ и ВТСС), так и применения средств активной защиты [71].

Параметрический канал утечки информации

Параметрический канал утечки информации используется для перехвата обрабатываемой в технических средствах информации путем их *«высокочастотного облучения»*. При воздействии облучающего электромагнитного поля на элементы ТСПИ происходит переизлучение электромагнитного поля. В ряде случаев возможна модуляция вторичного излучающего поля информационным сигналом. Для исключения взаимного влияния облучающего и переизлученного сигналов может использоваться их временное или частотное разделение. Например, для облучения ТСПИ могут использовать импульсные сигналы, в промежутках между которыми осуществляется прием переизлученных сигналов [71].

При переизлучении параметры сигналов изменяются. Поэтому данный канал утечки информации часто называют *параметрическим*.

Для перехвата информации по данному каналу применяют специальные высокочастотные генераторы с антеннами, имеющими узкие диаграммы направленности, и специальные радиоприемные устройства.

Информация после обработки в ТСПИ может передаваться по проводным каналам связи, где также возможен ее перехват.

1.3.2 Технические каналы утечки информации при передаче ее по каналам связи

Для передачи информации используют в основном КВ, УКВ, радиорелейные, тропосферные и космические каналы связи, а также кабельные и волоконно-оптические линии связи [71].

Работа любого электронного устройства основана на получении, обработке и передаче информации, представленной в виде электрических сигналов. В передаче электрического сигнала участвуют источник, средства передачи и приемник сигнала. Устройства передачи электрических сигналов от источника к приемнику называют *электромагнитными линиями связи* или кратко – *линиями связи*. Линии связи используют в качестве средства передачи энергию электрического поля, магнитного поля, электромагнитного поля излучения, электрические проводники и волноводы.

Каналы утечки информации за счет паразитных связей

Утечка информативного сигнала по цепям электропитания и слаботочных линий может происходить различными путями. Например, между двумя электрическими цепями, находящимися на некотором расстоянии друг от друга, могут возникнуть электромагнитные связи, создающие объективные предпосылки для появления информативного сигнала в цепях системы электропитания объектов вычислительной техники (ВТ). Эти процессы называются наводками, которые обеспечивают передачу энергии из одного устройства в другое, не предусмотренную схемными или конструктивными решениями [71].

Источниками наводки являются устройства, в которых обрабатывается информативный сигнал; приемниками – цепи электропитания, выступающие в качестве токопроводящей среды, выходящей за пределы контролируемой территории и одновременно с этим представляющие собой опасный канал утечки информации, обрабатываемой ПЭВМ и ЛВС.

Утечка информации при функционировании средств ВТ также возможна либо через непосредственное излучение и наведение информативных импульсов, циркулирующих между функционально законченными узлами и блоками, либо посредством высокочастотных электромагнитных сигналов, модулированных информативными импульсами и обладающих способностью самонаводиться на провода и общие шины электропитания через паразитные связи [71].

Объекты, излучающие сигналы, содержат источники сигнала. Если объект отражает поля внешних источников, то он является источником информации об объекте и в то же время является источником сигнала.

Может быть такой источник сигнала, который переписывает информацию с одного носителя на другой. Если источником сигнала является радиозакладка и первичным – речевой сигнал от говорящего человека. Мембрана является преобразователем акустического сигнала в электрический. Такой источник сигнала называется передатчиком [71].

Если источник сигнала применяется для обеспечения связи между санкционированными объектами, то такие источники называются

функциональными источниками сигнала. Существуют источники опасных сигналов – это источники, от которых могут распространяться несанкционированным образом сигналы защищаемой информации.

Источником сигналов могут быть любые объекты излучения.

Источниками опасных сигналов могут быть [71]:

1) акустоэлектрические преобразователи (пьезоэлектрические, емкостные, индуктивные);

2) излучатели низкочастотных сигналов (элементы РЭС, усилительные каскады, генераторы, ПЭВМ);

3) излучатели высокочастотных сигналов;

4) паразитные связи и наводки (гальванические, индуктивные, емкостные).

Паразитная связь обусловлена не предусмотренной электрической схемой и конструкцией изделия связью между элементами устройства или устройством и внешней средой, приводящая к появлению помехи.

Помехи представляют собой электрические сигналы, не предусмотренные электрической схемой изделия. Помехи подразделяются на шумы и наводки. Наводки – это помехи, возникающие из-за паразитных связей.

Шумы – это электрические сигналы (помехи), обусловленные в электронных приборах их внутренними свойствами независимо от наличия внешних связей и сигналов [71].

Паразитными называют элементы, появившиеся в результате неидеальности практической реализации электрической схемы из-за невозможности создания проводников и линий связи, не обладающих сопротивлением, индуктивностью и емкостью.

Канал связи может являться как источником, так и приемником помех. Если два канала связи имеют взаимную паразитную связь, то и наводки, а, следовательно, и утечка информационных сигналов, возникают в обоих каналах взаимно. Уровень наводок и их влияние на работу канала связи зависит от относительного уровня сигналов в каналах.

Электрические каналы утечки информации

Электрический канал утечки информации при ее передаче по линиям связи может быть образован путем непосредственного контактного подключения к кабельным линиям аппаратуры перехвата. Для повышения скрытности аппаратура перехвата подключается к линии через специальные согласующие устройства, снижающие вносимое сопротивление и падение напряжения на линии. Некоторые кабели связи для защиты от подключения устройств перехвата снабжаются воздухонепроницаемой оболочкой, внутри которой поддерживается избыточное контролируемое давления воздуха. В этом случае средства перехвата должны иметь возможность компенсации снижения давления воздуха при подключении к кабелю [71].

Этот канал наиболее часто используется для перехвата низкочастотных телефонных сигналов в линиях связи в местах свободного доступа. В дальнейшем перехватываемая информация может быть записана на диктофон или передана по радиоканалу. Если подобные устройства содержат радиопередатчики для

ретрансляции перехваченной информации, то их называют телефонными закладками.

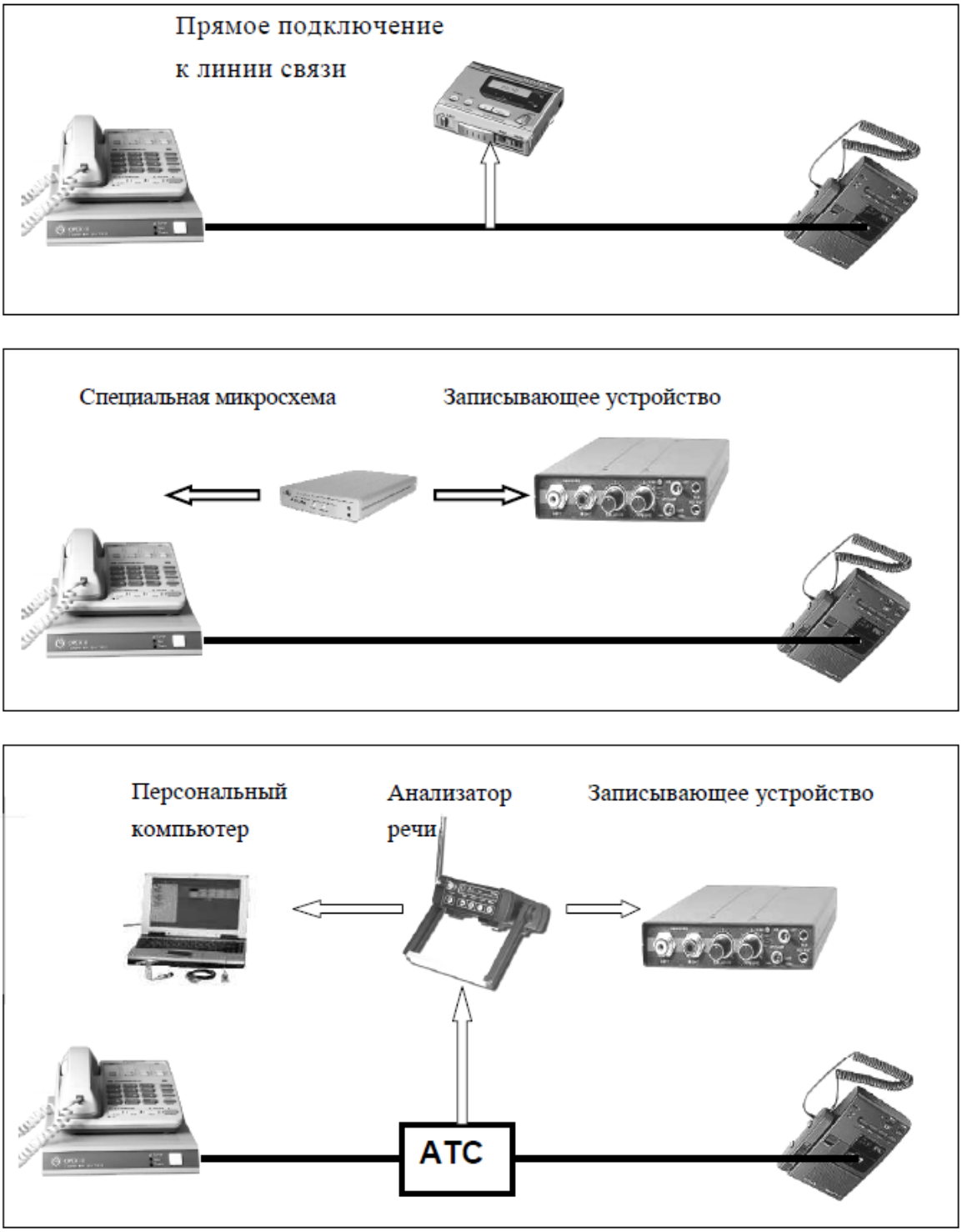


Рисунок 1.4 - Схемы возможных вариантов подключения к телефонной линии без использования радиоканала

Контроль и прослушивание телефонных каналов связи

Одним из основных способов несанкционированного доступа к информации частного и коммерческого характера является прослушивание телефонных

переговоров. Для прослушивания телефонных переговоров используются следующие способы подключения [71]:

- Параллельное подключение к телефонной линии. В этом случае телефонные радиоретрансляторы (телефонные закладки) труднее обнаруживаются, но требуют внешнего источника питания.

- Последовательное включение телефонных радиоретрансляторов в разрыв провода телефонной линии. В этом случае питание телефонного радиоретранслятора осуществляется от телефонной линии и на передачу он выходит с момента подъема телефонной трубки абонементом.

Подключение телефонного радиоретранслятора может осуществляться как непосредственно к телефонному аппарату, так и к любому участку линии от телефона абонента до АТС. В настоящее время существуют телефонные радиоретрансляторы, позволяющие прослушивать помещение через микрофон лежащей трубки. Для этого на один провод телефонной линии подключается генератор высокочастотных колебаний, а к другому – амплитудный детектор с усилителем. Высокочастотные колебания проходят через микрофон или элементы телефонного аппарата, обладающие «микрофонным эффектом», и модулируются акустическими сигналами прослушиваемого помещения. Модулированный высокочастотный сигнал демодулируется амплитудным детектором и после усиления прослушивается или записывается [71].

Дальность действия такой системы из-за затухания ВЧ сигнала в двухпроводной линии не превышает нескольких десятков метров. Имеются системы прослушивания телефонных разговоров, которые не требуют непосредственного электронного соединения с телефонной линией. Эти системы основаны на индуктивном способе съема информации при помощи специальных катушек. Они сложны и громоздки, поскольку содержат несколько каскадов усиления слабого низкочастотного сигнала и обязательный внешний источник питания. Поэтому такие системы не нашли широкого практического применения.

Для приема информации от телефонных радиотрансляторов применяют такие же приемники, как в акустических устройствах съема информации по радиоканалу.

Непосредственное подключение к телефонной линии. Непосредственное подключение к телефонной линии – наиболее простой и надежный способ получения информации. В простейшем случае применяется трубка ремонтника-телефониста, подключаемая к линии в распределительной коробке, где производится разводка кабелей. Чаще всего это почерк «специалистов» нижнего звена уголовного мира (верхнее звено оснащено аппаратурой не хуже государственных секретных служб) [71].

Прослушивание помещений через микрофон телефонного аппарата. В этом случае телефонная линия используется не только для передачи телефонных сообщений, но и для прослушивания помещения. Микрофон является частью электронной схемы телефонного аппарата: он либо соединен с линией (через отдельные элементы схемы) при разговоре, либо отключен от нее, когда телефонный аппарат находится в ожидании вызова (трубка находится на аппарате). На первый взгляд, когда трубка лежит на аппарате, нет никакой

возможности использовать микрофон в качестве источника съема информации. На самом деле это не так [71].

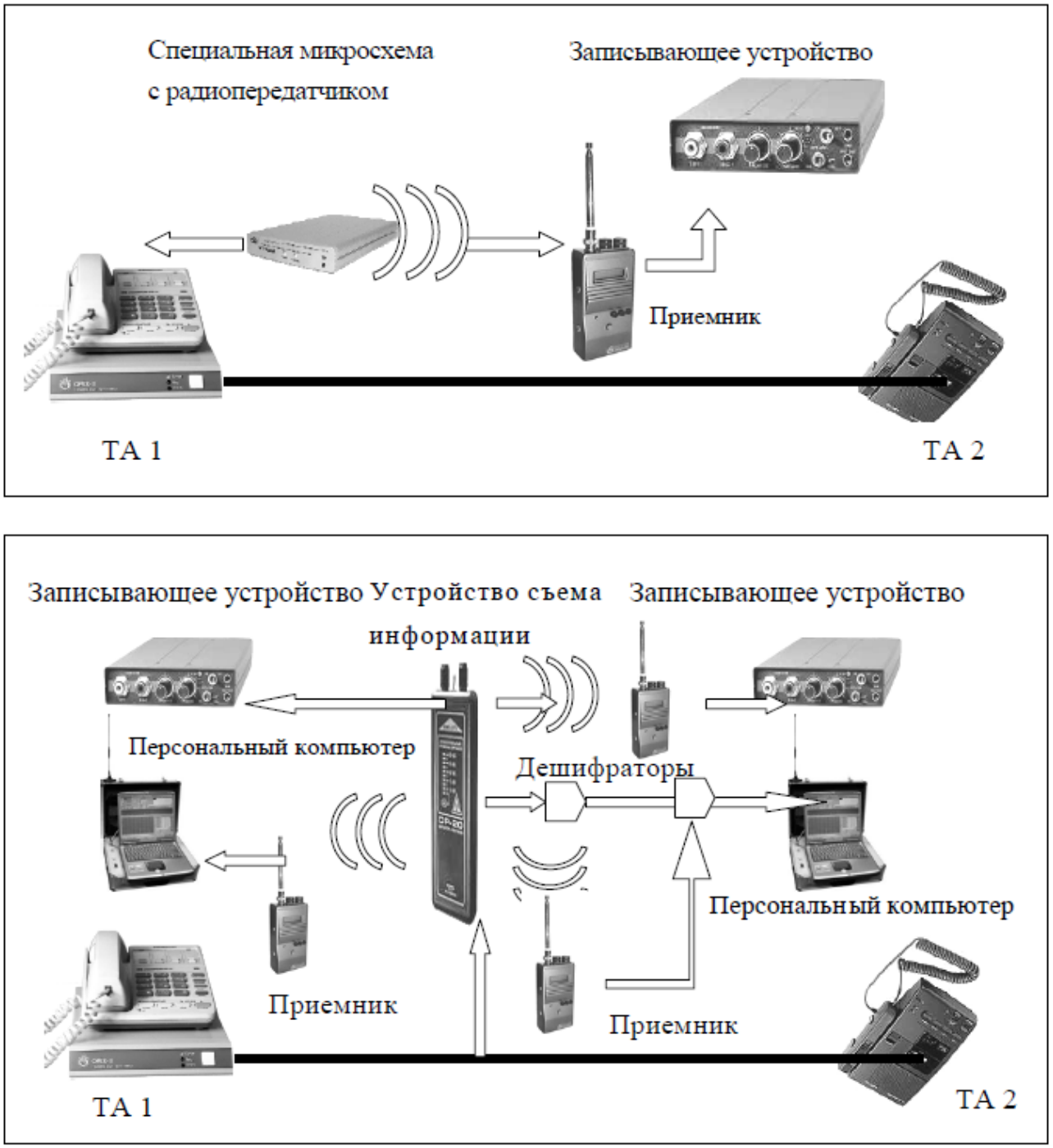


Рисунок 1.5 - Схемы возможных вариантов подключения к телефонной линии с использованием радиоканала

На рис. 1.6 приведена схема прослушивания помещения способом, называемым высокочастотным навязыванием. Этот способ аналогичен способу высокочастотной накачки и состоит в следующем.

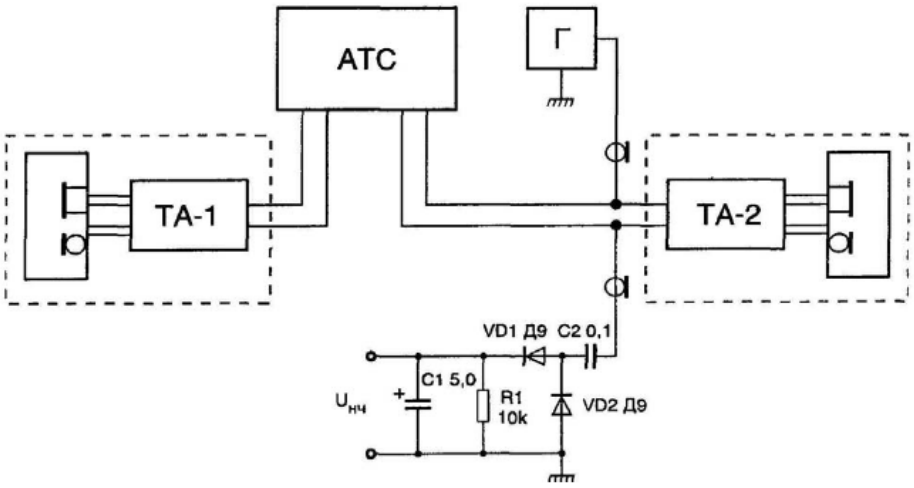


Рисунок - 1.6 Прослушивание через микрофон телефонного аппарата

На один из проводов телефонной линии, идущий от АТС к телефонному аппарату ТА-2, подаются колебания частотой 150 кГц и выше от генератора Г. К другому проводу линии подключается детектор, выполненный на элементах Cl, С2, VD1, VD2 и R1. Корпус передатчика (генератор Г) и приемника (детектор) соединены между собой или с общей землей, например с водопроводной трубой.

Недостаток этого метода состоит в том, что его случайно может обнаружить всякий, кто позвонит по тому же номеру, а также необъяснимая занятость контролируемой линии для других абонентов [71].

Электромагнитные каналы утечки информации

Электромагнитные излучения передатчиков средств связи, модулированные информационным сигналом, могут перехватываться с использованием стандартных технических средств радиоразведки. Этот электромагнитный канал перехвата информации широко используется для прослушивания телефонных разговоров, ведущихся по радиотелефонам, сотовым телефонам или по радиорелейным и спутниковым линиям связи [71].

Индукционный канал утечки информации

Данный канал чаще всего используется для съема информации с симметричных высокочастотных кабелей. Непосредственное электрическое подключение аппаратуры перехвата легко обнаруживается специальными контролирующими средствами. Индукционный канал перехвата, не требующий контактного подключения к каналам связи, свободен от этого недостатка. Электромагнитное поле, возникающее вокруг проводников кабеля под действием информационных токовых сигналов, наводит в специальных индукционных датчиках адекватные информационные сигналы [71].

Современные индукционные датчики способны снимать информацию с кабелей, защищенных не только изоляцией, но и двойной броней из стальной ленты и стальной проволоки, плотно обвивающих кабель.

1.3.3 Технические каналы утечки речевой информации

Все средства акустической разведки в своей основе используют микрофоны различных типов и назначения. К основным характеристикам микрофонов относятся: чувствительность, частотная характеристика, характеристика направленности и уровень собственного шума [43].

Микрофоны по принципу электромеханического преобразования делятся на *электродинамические*, *электростатические*, *электромагнитные и релейные*.

Электродинамические микрофоны по конструкции механической системы делятся на *катушечные* (динамические) и *ленточные*. Электростатические делятся на к*онденсаторные*, в том числе и электретные, и *пьезомикрофоны*. Электромагнитные делятся на односторонние и дифференциальные. Релейные делятся на угольные и транзисторные [74].

По акустическим характеристикам микрофоны делятся на приемники давления, приемники градиента давления, комбинированные и групповые. Особенностью приемника давления является то, что его подвижная механическая система (диафрагма) подвержена воздействию звуковых волн только с одной стороны.

У приемника градиента давления подвижная механическая система открыта для звуковых волн с обеих сторон, поэтому на неё действует разность давлений волн падающих на фронтальную поверхность диафрагмы и огибающей её с тыльной стороны.

Для получения различных форм характеристик направленности обычно комбинируют приемники давления и градиента давления.

Динамический микрофон представляет собой катушку, находящуюся в магнитном поле кольцевого магнита и жестко связанную с диафрагмой.

Конденсаторный микрофон – это конденсатор, у которого один из элементов массивный, а другой – тонкая натяжная мембрана. При колебаниях мембраны емкость конденсатора изменяется, а заряд q остается неизменным (конденсатор в цепи постоянного тока с последовательно включенным большим сопротивлением нагрузки $R_н$ не успевает разряжаться). В результате изменяется напряжение на конденсаторе в соответствии с выражением

$$i = C\frac{du_C}{dt}. \qquad (1.1)$$

Напряжение снимается с сопротивления нагрузки.

В электретном микрофоне поляризующее напряжение образовано предварительной электризацией одного из электродов, изготовляемого изполимеров или керамических поляризующихся материалов. Такой электрод имеет металлическое покрытие, которое является электродом конденсатора, а электрет служит лишь источником поляризующего напряжения.

Из-за уменьшения поляризации электрета с течением времени требуется или замена, или повторная поляризация через несколько лет. По характеристикам

такой микрофон не отличается от конденсаторного, но не требует источника напряжения.

В пьезомикрофонах используется явление пьезоэффекта. При деформации пластинки из кварца или пьезокерамиков (титан, барий и др.) происходит её поляризация, т.е. концентрация зарядов на плоскостях. Пьезомикрофоны относятся к электростатическому типу микрофонов и не требуют источника питания. Они сходны по свойствам с электретными микрофонами.

Направленные микрофоны

Направленные микрофоны предназначены прежде всего для акустического контроля источников звуков на открытом воздухе. В таких ситуациях решающим фактором оказывается удаленность источника звука от направленного микрофона, что приводит к значительному ослаблению уровня контролируемого звукового поля (кроме того, при большой дистанции становится заметным ослабление звука из-за разрушения пространственной когерентности поля вследствие наличия естественных рассеивателей энергии, например средне- и крупномасштабных турбулентностей атмосферы, создающих помехи при ветре) [43].

Так, на дистанции 100 м давление звука ослабляется на величину не менее 40 дБ (по сравнению с дистанцией 1 м), и тогда степень громкости обычного разговора в 60 дБ окажется в точке приема не более 20 дБ. Такое давление существенно меньше не только уровня реальных внешних акустических помех, но и пороговой акустической чувствительности обычных микрофонов.

В отличие от обычных, направленные микрофоны должны иметь[43]:

- Высокую пороговую акустическую чувствительность, чтобы ослабленный звуковой сигнал превышал уровень собственных (в основном тепловых) шумов приемника. Даже при отсутствии внешних акустических помех это является необходимым условием контроля звука на значительном расстоянии от источника.

Виды направленных микрофонов. Существует четыре вида направленных микрофонов [43]:

- параболические;
- плоские акустические фазированные решетки;
- трубчатые, или микрофоны «бегущей» волны;
- градиентные.

Параболический микрофон состоит из отражателя звука параболической формы, в фокусе которого расположен обычный (ненаправленный) микрофон. Отражатель изготавливается как из оптически непрозрачного, так и прозрачного материала.

Величина внешнего диаметра параболического зеркала может находиться в пределах от 200 до 500 мм. Принцип работы этого микрофона поясняется на рис.1.7.

Звуковые волны с осевого направления отражаются от параболического зеркала и суммируются в фазе в фокальной точке *A*. За счет этого эффекта возникает усиление звукового поля. Чем больше диаметр зеркала, тем большим усилением характеризуется микрофон. Если направление волны звука не осевое,

то сложение отраженных от различных частей параболического зеркала звуковых волн в точке *A* произойдет со сдвигом по фазе и усиление микрофона будет меньшим. Ослабление тем сильнее, чем больше угол прихода звука по отношению к оси. Параболический микрофон является примером высокочувствительного, но слабонаправленного микрофона.

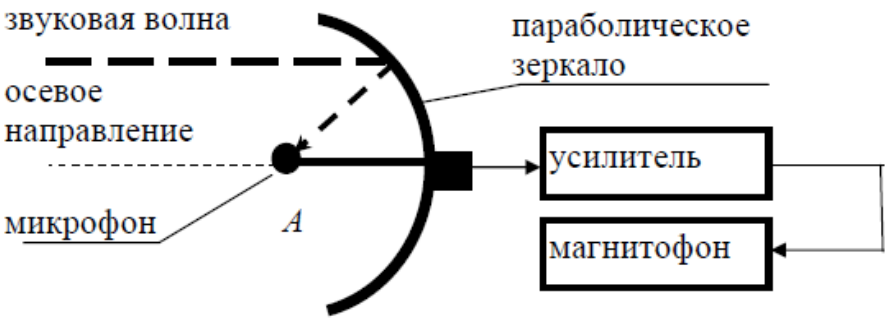


Рисунок 1.7 - Параболический микрофон

Плоские фазированные решетки обеспечивают одновременный прием звукового поля в дискретных точках некоторой плоскости, перпендикулярной к направлению на источник звука (рис. 1.8).

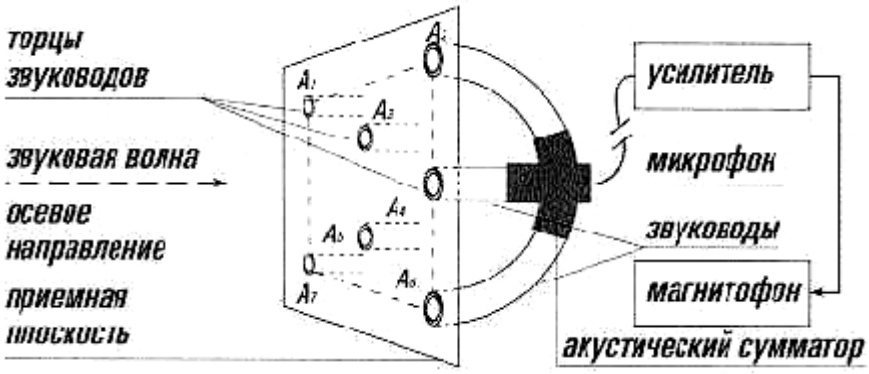


Рисунок 1.8 - Плоская фазированная решетка

Трубчатый микрофон представляет собой звуковод в форме жесткой полой трубки диаметром 10–30 мм со специальными щелевыми отверстиями, размещенными рядами вдоль оси звуковода, с круговой геометрией расположения для каждого из рядов (рис. 1.9). При приеме звуковой волны с осевого направления будет происходить сложение в фазе сигналов, проникающих в звуковод через все щелевые отверстия, в силу равенства скоростей осевого распространения звука вне трубки и внутри нее. Когда же звук приходит под некоторым углом к оси микрофона, то это ведет к неравенству длин путей распространения звуковых волн и фазовому рассогласованию, в результате чего снижается чувствительность приема. Обычно длина трубчатого микрофона находится в пределах от 15–230 мм до 1 м. Чем больше его длина, тем сильнее подавляются помехи с боковых и тыльного направлений.

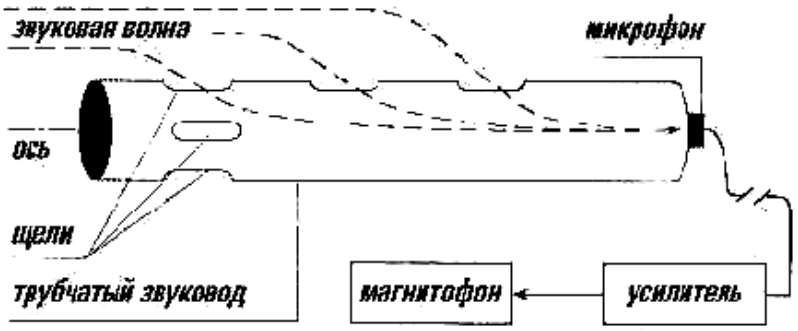


Рисунок 1.9 - Трубчатый микрофон

Примеры технической реализации направленных микрофонов приведены ниже.

Монокуляр с направленным микрофоном «СУПЕР УХО-100» (рис. 1.10) обеспечивает 8 кратное увеличение. Параболический отражатель способствует созданию узкой диаграммы направленности микрофона.

Рисунок 1.10 - Монокуляр с направленным микрофоном «СУПЕР УХО-100»

Имеется возможность аудиозаписи на встроенный диктофон в течение 12 сек. Дальность действия микрофона до 100 м. Питание 9 В от батареи типа «Крона». Наушники входят в комплект поставки.

Направленный микрофон «Yukon» (рис. 1.11) – это высококачественный профессиональный прибор для прослушивания и записи звуковых сигналов от удаленных объектов. Микрофон имеет штативное гнездо 1/4 дм, которое позволяет установить его на стандартный штатив [79].

Рисунок 1.11 - Направленный микрофон «Yukon»

Данный микрофон имеет узкую диаграмму направленности – суперкардиоиду. Изготовленный по новейшей технологии направленный микрофон «Yukon» является высокочувствительным конденсаторным микрофоном, позволяющим услышать звуки на расстоянии до 100 м.

Микрофон имеет автономное питание, обеспечивающее непрерывную работу в течение 300 ч. Эффективная ветрозащита позволяет значительно снизить фон от воздушных потоков.

В приборе ночного видения с направленным микрофоном NVS 2,5×42 (рис. 1.12) впервые реализована идея одновременного визуального и акустического контроля в условиях естественной ночной освещенности за объектами, расположенными на значительном удалении от наблюдателя 80].

Рисунок 1.12 - Направленный микрофон с прибором ночного видения NVS 2,5×42

В приборе ночного видения используется оптическая схема, базирующаяся на электронно-оптических преобразователях нулевого поколения. Благодаря оптимально рассчитанной кратности (2,5) и светосиле, прибор обеспечивает высокое качество изображения. Наличие фотоадаптера позволяет проводить фото- и видео съемку в ночных условиях. Мощный ИК-осветитель дает возможность вести наблюдение в условиях полной темноты.

С помощью направленного микрофона можно осуществлять прослушивание и запись различных звуковых сигналов на расстоянии до 100 м.

Проводные системы, портативные диктофоны и электронные стетоскопы

Средства акустической разведки выбираются в зависимости от возможности доступа в контролируемые места.

Микрофоны всех типов имеют диапазон чувствительности от 6 до 10 мВ/Па и в состоянии регистрировать голос человека нормальной громкости на расстоянии 10–15 м, а некоторые образцы – до 20 м, в частотном диапазоне 100 Гц – 20 кГц.

Если имеется возможность постоянного проникновения в контролируемые помещения, в нем заранее могут быть установлены миниатюрные микрофоны, линии передачи сигналов которых выводятся в специальное помещение, где находится злоумышленник и установлена регистрирующая аппаратура. Длина линии передачи сигнала может достигать 5000 м. Такие системы называются проводными системами [43].

Для обеспечения скрытности микрофонов последние выпускаются в сверхминиатюрном исполнении (диаметр менее 2,5 мм) и камуфлируются под различные предметы.

Для повышения качества перехваченных разговоров микрофоны устанавливаются возможно ближе к местам проводимых разговоров, а улучшение чувствительности может быть обеспечено подключением микрофонов к предусилителям.

В качестве регистрирующей аппаратуры используются магнитофоны и диктофоны с длительным временем записи (до 16 ч). Для улучшения качества записи и скрытности всё чаще используются цифровые магнитофоны.

Цифровой бескинематический магнитофон «U-7102» показан на рис. 1.13. В аппарате для преобразования речевого сигнала в цифровой поток используется кодер V-16 [81]. Алгоритм обеспечивает длительное время записи информации без применения программного сжатия и позволяет получать высокое качество речевой информации в сложных акустических условиях. Магнитофон обеспечивает высокое качество записи информации при работе систем подавления диктофонов и в условиях постановки целенаправленных акустических помех.

Рисунок 1.13 - Цифровой бескинематический магнитофон «U-7102»

Блок воспроизведения некоторых магнитофонов позволяет подключение к компьютеру. Для управления воспроизведением применяют программное обеспечение, которое позволяет:

- моментально получить доступ к любому ранее записанному фрагменту в выбранном для прослушивания файле;
- отсортировать записанные разговоры по различным признакам (время начала, длительность, номер канала с одним из микрофонов подслушивания);
- выделять и копировать в новый файл как разговоры полностью, так и фрагменты из них по выбору и в любом порядке;
- переписывать созданные файлы фрагментов на другие носители.

Эквалайзеры представляют собой специальные устройства с набором различных фильтров: фильтров верхних и нижних частот, полосовых, основных и

др. Эти фильтры включаются по определенной программе в зависимости от характера искажений сигнала и помех и повышают разборчивость речи.

Наряду с эквалайзерами для повышения разборчивости речи используются специальные программно-аппаратные комплексы. Обычно в состав подобных комплексов входят:

- устройство ввода/вывода речевых сигналов, включающее АЦП и ЦАП;
- плата специализированного сигнального процессора, предназначенного для реализации в реальном масштабе времени процедур обработки речевых сигналов, в частности шумоподавления;
- пульт управления;
- компьютер;
- программное обеспечение и другие средства.

Если не удается проникнуть в контролируемое помещение, но имеется возможность проникновения в соседнее помещение, то для сбора речевой информации используются электронные стетоскопы, преобразующие акустические колебания в твердых телах (стенах, потолках, полах, трубах) в электрические сигналы. Чувствительным элементам электронных стетоскопов является контактный микрофон (чаще всего на основе пьезоэлемента), соединенный с усилителем. Стетоскоп представляет собой вибродатчик, усилитель и головные телефоны. Размеры датчика, на примере устройства DTI, составляют 2,2×8 см. С помощью подобных устройств можно осуществлять прослушивание разговоров через стены толщиной до 1 м. Стетоскоп может оснащаться проводным, радио или другим каналом передачи информации. Достоинством стетоскопа является трудность его обнаружения при установке в соседних помещениях [71].

Имеются стетоскопы, у которых чувствительный элемент, усилитель и радиопередатчик имеют общий корпус. Примером такого устройства является стетоскоп АД-50. Этот компактный стетоскоп позволяет не только прослушивать разговоры через стены, оконные рамы, двери, но и передавать информацию по радиоканалу. Он имеет высокую чувствительность и обеспечивает хорошую разборчивость речевого сигнала. Его несущая частота составляет 470 МГц, дальность передачи – до 100 м.

На рис. 1.14 показан стереофонический стетоскоп СС 021, предназначенный для анализа виброакустической защиты строительных конструкций. Датчики стетоскопа имеют чувствительность не хуже 10^{-5} g [82].

Рисунок 1.14 - Стетоскоп стереофонический СС 021

Современные электронные стетоскопы имеют коэффициент усиления до 30000 и способны фиксировать слабые звуковые колебания (шорохи, тиканье часов) через бетонные стены толщиной 50–100 см [74].

Радиомикрофоны

Принцип действия радиозакладок микрофонного типа основан на преобразовании акустических сигналов с помощью микрофона в электрические сигналы и передачи их по радиоканалу на приемное устройство. Такие подслушивающие устройства получили наибольшее распространение благодаря простоте исполнения и дешевизне. В качестве источника питания могут служить автономные источники питания, электрическая и телефонная сети [71].

Микрофон определяет зону акустической чувствительности (до 20–30 м), радиопередатчик – дальность действия радиолинии. Важными параметрами с точки зрения дальности действия для передатчика являются мощность, стабильность несущей частоты, диапазон частот, вид модуляции.

По конструктивному исполнению радиозакладки могут быть простыми, работающими как обычные передатчики с амплитудной или частотной модуляцией. В то же время радиозакладки могут быть и весьма сложными: иметь в своем составе устройства дистанционного управления, автоматиче-ского включения при определенных условиях, системы накопления информации и передачи ее короткими сериями на повышенных скоростях и т.д.

Наличие такого большого количества моделей радиомикрофонов объясняется тем, что в различных ситуациях требуется определенная модель.

Радиозакладки, устанавливаемые в телефонную линию, используют её и в качестве источника питания и в качестве антенны. Некоторые позволяют прослушивать только телефонные разговоры, а некоторые ещё и разговоры в помещении, где установлен телефонный аппарат. При разговоре акустические волны воздействуют на телефонный капсюль и он передает сигналы по сети, даже если трубка положена. При поднятии трубки закладка переходит в режим прослушивания телефонного разговора. Такие закладки удобны тем, что можно слушать, например, и телефон и квартиру, даже не проникая в неё, достаточно подключить такую закладку к телефонной линии в подъезде. Подключаются телефонные закладки к линии по параллельной схеме [71].

Так как питается такая закладка от телефонной линии, то время её работы практически не ограничено.

Гидроакустические датчики

Звуковые волны распространяются в воде с очень небольшим затуханием. Этот принцип можно применять для их регистрации, используя жидкость, находящуюся в системах водоснабжения и канализации. Такую информацию можно получить в пределах здания, но радиус прослушивания будет очень сильно зависеть от уровня шумов, особенно в водопроводе. Ещё более эффективным будет использование гидроакустического передатчика, установленного в батарее прослушиваемого помещения [71].

СВЧ- и ИК-передатчики

Для повышения скрытности передачи речевой информации используется инфракрасный канал. В качестве передатчика звука от микрофона используется

полупроводниковый лазер. В качестве примера приведем устройство TRM-1830. Дальность действия днем составляет 150 м, ночью – 400 м, время непрерывной работы – 20 ч. Габариты не превышают 26×22×20 мм. К недостаткам подобной системы можно отнести необходимость прямой видимости между передатчиком и приемником и влияние помех на качество передачи сигналов [71].

Повысить скрытность получения информации можно также с помощью использования канала СВЧ в диапазоне более 10 ГГц. Передатчик, выполненный на диоде Ганна, может иметь очень небольшие габариты.

К преимуществам такой системы можно отнести отсутствие помех, простоту и отсутствие в настоящее время эффективных средств контроля.

К недостаткам следует отнести необходимость прямой видимости, хотя и в меньшей степени, так как СВЧ-сигнал может все-таки огибать небольшие препятствия и проходит хотя и с ослаблением сквозь тонкие диэлектрики, например, шторы на окнах.

Виброакустические технические каналы утечки речевой информации

Перехват акустических сигналов по виброакустическим техническим каналам возможен [71]:

- электронными стетоскопами;
- стетоскопами с передачей информации по радиоканалу;
- стетоскопами, подключенными к устройствам передачи информации по оптическому каналу в ИК-диапазоне длин волн;
- стетоскопами, объединенными с устройствами передачи информации по трубам водоснабжения, отопления, металлоконструкциям и т.п.

Акустоэлектрические каналы утечки речевой информации

Перехват акустических колебаний возможен [71]:

- через ВТСС, обладающих «микрофонным эффектом», путем подключения к их соединительным линиям;
- через ВТСС путем «высокочастотного навязывания».

Оптико-электронный технический канал утечки речевой информации

Оптико-электронный технический канал утечки информации образуется путем облучения лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей (стекол, картин, зеркал).

Схема простейшего лазерного микрофона показана на рис. 1.15. Звуковая волна, генерируемая источником акустического сигнала, падает на границу раздела воздух-стекло со стороны помещения и создает вибрацию (отклонения поверхности стекла от исходного положения). Эти отклонения вызывают дифракцию света, отражающегося от внешней стороны стекла [71].

Если размеры падающего оптического пучка малы по сравнению с длиной «поверхностной» волны, то в составе различных компонент отраженного света будет доминировать дифракционный пучок нулевого порядка. В этом случае, во-первых, фаза световой волны оказывается промодулированной по времени с частотой звука и однородной по сечению пучка, а во-вторых, пучок «качается» с частотой звука вокруг направления зеркального отражения.

Отраженное лазерное излучение принимается от сплиттера чувствительным приемником лазерного излучения (детектором). Применение сплиттера (делителя

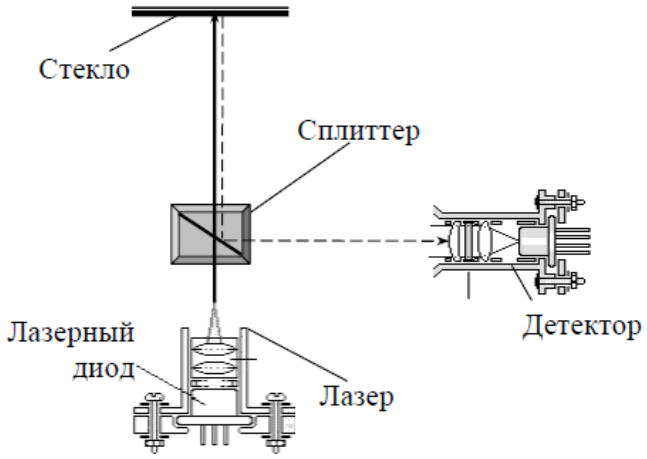


Рисунок 1.15 - Схема простейшего лазерного микрофона

пучка) позволяет свести падающий и отражённый луч в одну точку. При демодуляции отраженного лазерного излучения выделяется речевая информация.

Лазер и приемник образуют сложную лазерную акустическую локационную систему («лазерный микрофон»), работающую в ближнем инфракрасном диапазоне волн. Реально лазер, сплиттер и детектор могут быть совмещены в одном устройстве.

В открытых публикациях сообщается, что, например, система SIPE LASER 3-DA SUPER производства США использует в качестве источника излучения гелий-неоновый лазер. Наведение прибора на объект осуществляется с помощью телескопического визира, а съем речевой информации с оконных рам с двойным остеклением обеспечивается с расстояния до 250 м хорошим качеством. Другое лазерное устройство HPO150 фирмы HEWLETT PACKARD обеспечивает регистрацию разговоров, ведущихся в помещениях, на дальности до 1000 м [71].

Качество принимаемой информации зависит от следующих факторов:

- параметров используемого лазера (длина волны, мощность, когерентность и т. д.);
- параметров фотоприемника (чувствительность и избирательность фотодетектора, вид обработки принимаемого сигнала и т.д.);
- параметров атмосферы (рассеяние, поглощение, турбулентность, уровень фоновой засветки и т.д.);
- качества обработки зондируемой поверхности (шероховатости и неровности, обусловленные как технологическими причинами, так и воздействием среды);
- уровня фоновых акустических шумов;
- уровня перехваченного речевого сигнала.

Параметрические технические каналы утечки речевой информации

Перехват акустических сигналов в параметрических технических каналах утечки информации возможен:

- путем приема и детектирования электромагнитных излучений (ЭМИ) на частотах ВЧ генераторов ТСПИ и ВТСС, модулированных информационным сигналом;

Модулированные информационным сигналом высокочастотные колебания излучаются в окружающее пространство и могут быть перехвачены и детектированы специальными приемниками средств радиоразведки.

Параметрический канал утечки информации может быть организован также и при высокочастотном облучении помещения с установленными полуактивными закладными устройствами, некоторые характеристики которых модулируются по закону изменения акустического сигнала. Так, например, при облучении мощным направленным высокочастотным сигналом помещения, в котором находится такое закладное устройство, в последнем при взаимодействии облучающего электромагнитного поля со специальными элементами закладки (например, четвертьволновым вибратором или объемным резонатором) происходит образование вторичных радиоволн, т.е. переизлучение электромагнитного поля. Полуактивные закладные устройства подобного типа могут обеспечивать амплитудную, фазовую или частотную модуляцию переотраженного сигнала по закону изменения речевого сигнала. Для перехвата информации по данному каналу кроме закладного устройства необходимы специальный передатчик с направленной антенной и приемник [71].

Примером полуактивного закладного устройства может служить аудио-транспондер (рис. 1.16). Он начинает работать только тогда, когда происходит его облучение высокочастотным зондирующим сигналом. Транспондер трудно обнаружить, так как он может быть вмонтирован в стену.

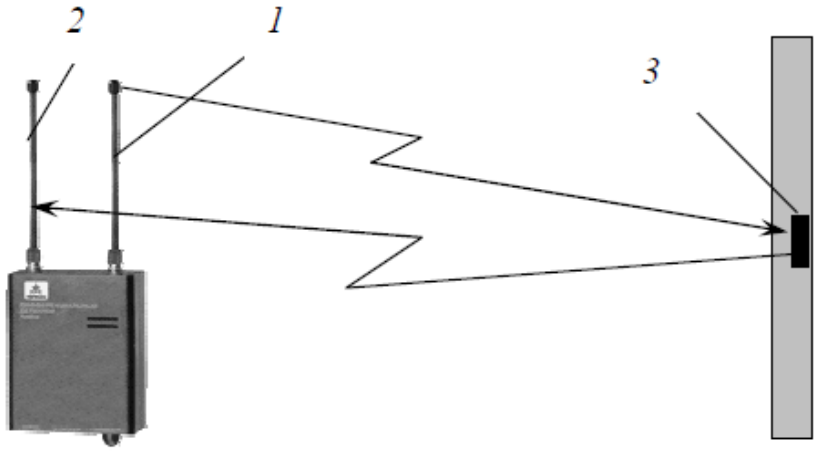


Рисунок 1.16 - Схема аудио-транспондера: *1* – антенна облучающего передатчика; *2* – антенна приемника; *3* – полуактивная радиозакладка в стене

Приемник транспондера принимает зондирующий сигнал и подает его на узкополосный частотный модулятор. Модулирующим является сигнал, поступающий непосредственно от микрофона или от микрофонного усилителя. Модулированный высокочастотный сигнал переизлучается со смещением по

частоте относительно опорной. Переизлученный сигнал принимается приемником, в котором осуществляется его демодуляция.

Из-за отсутствия специального источника питания время работы транспондера не ограничено.

1.3.4 Технические каналы утечки видовой информации

Визуальное наблюдение является самым давним и очень эффективным методом сбора информации. Как известно, высокий уровень охраны субъекта или объекта предполагает значительное насыщение пространства вокруг охраняемого самыми разнообразными техническими средствами и многочисленными сотрудниками охраны. Данное обстоятельство осложняет доступ к объекту и получение информации о деятельности физических лиц. Поэтому для выявления интересующих подробностей в 99% случаев из ста применяется разнообразная оптика.

Задача своевременного выявления и обнаружения ведущегося оптического наблюдения становится, таким образом, одной из важнейших при проведении как профилактических, так и специальных защитных и охранных мероприятий. Своевременное обнаружение факта несанкционированного наблюдения дает возможность установить, с какой целью оно проводится и определить угрозу, которая может исходить от наблюдающего за тем или иным объектом, персоной или группой лиц.

Для получения информации широко используется скрытая фото - и видеосъемка.

В настоящее время для сбора информации могут использоваться миниатюрные скрытые и специальные (камуфлированные под обычные предметы) фото- и видеокамеры. На рис. 1.17 показана одна из микрофотокамер – закамуфлированная цифровая микрофотокамера Minox DD1 [71].

Рисунок 1.17 - Закамуфлированная цифровая микрофотокамера Minox DD1

Фото- и видеокамеры бывают:

- миниатюрные (скрытые). Встраиваются в бытовую технику и передают видеоинформацию по кабелю или по ВЧ каналу при помощи телевизионного передатчика;

- специальные, т.е. замаскированные под бытовые предметы, например, пачку сигарет, кейс, книгу, наручные часы и т.п.

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

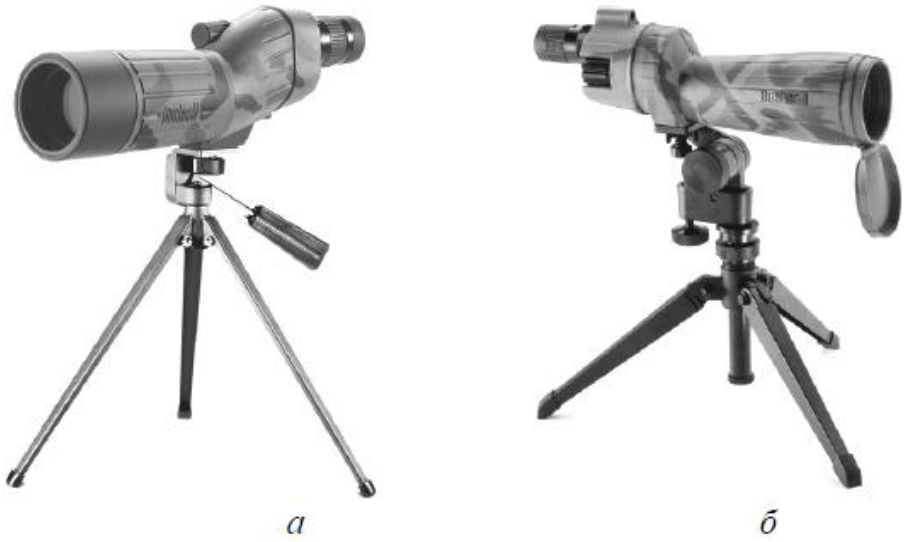
- миниатюрными объективами, предназначенными для съемки через отверстия небольшого диаметра (до 5 мм);

- телескопическими объективами, позволяющими вести съемку с дальних расстояний. Такие объективы обладают высокой кратностью увеличения (до 1,5 тыс. крат);

- камуфляжными объективами, используемыми для скрытой съемки из различных бытовых предметов, например из кейсов;

- объективами, совмещенными с приборами ночного видения (с инфракрасной подсветкой) и предназначенными для проведения съемки в темное время суток.

Спецслужбы давно и широко применяют различные оптические приборы для скрытного наблюдения и регистрации информации в дневных и ночных условиях при любой погоде. Для видеонаблюдения в дневное время применяются традиционные оптические приборы: бинокли, монокуляры, подзорные трубы, телескопы и др. На рис. 1.18 показаны самые популярные модели зрительных труб фирмы «Bushnell» – «Sentry 18-36×50» и «Spacemaster 20-45×60». Все линзы и призмы этих труб имеют многослойное просветляющее покрытие, которое обеспечивает хорошую светопередачу и яркое, насыщенное изображение. Линзы труб защищены от дождевых капель и не запотевают ни при каких условиях [71].



а *б*

Рисунок 1.18 - Зрительные трубы «Bushnell» – «Sentry 18-36×50» (*а*) и «Spacemaster 20-45×60» (*б*)

Для наблюдения за объектами на значительном расстоянии используются специальные телескопы. Например, телескоп прибора РК 6500 позволяет опознать автомобиль на расстоянии до 10 км [71].

Для ведения разведки ночью находят применение специальные телевизионные камеры (рис. 1.19), работающие при низком уровне освещённости, приборы ночного видения (ПНВ) и тепловизионные приборы (ТПВ).

На практике наиболее широко применяются приборы на основе оптикоэлектронных приборов (ОЭП) второго поколения. Такие приборы содержат микроканальную пластинку, представляющую собой диск с большим числом микроскопических каналов. Каждый канал является миниатюрным усилителем вторичной эмиссии электронов, испускаемых катодом ОЭП. Приборы обеспечивают возможность регистрации изображения на фото- и видеокамеры. Они обладают высоким усилением (до 50000), устойчивостью к засветкам, например фар автомашин, равномерным по полю разрешением и небольшими габаритами. Принцип их действия основан на приёме отражённого местными предметами оптического ИК-излучения и многократного его усиления и преобразованиея в видимое изображение [47].

Рисунок 1.19 - Видеокамеры Pelco

Современные приборы ночного видения работают при освещённости менее 0,01лк. Например, для прибора ночного видения «Ворон-3» пороговый уровень освещенности для визуального наблюдения составляет 0,001 лк, а для фотографирования – 0,01 лк. Разрешающая способность в этих условиях – не менее 8 линий на мм.

Комплект маскирования видеоизображения «VideoLock» (рис. 1.20) предназначен для маскирования видеоизображения при передаче его по проводным или радиоканалам. В комплекте применены новейшие цифровые технологии для передачи видеоизображения по проводным и радиоканалам.

Комплект характеризуется следующими свойствами:

- простота использования;
- метод маскировки: переворот и разрезание видеострок;
- помехи, возникающие при передаче видеоизображения по радиоканалу, не оказывают влияния на качество восстановленного изображения;
- изделия выполнены в виде модулей и предназначены для дальнейшей установки в приборы и оборудование;
- совместим с любым телевизионным оборудованием;
- наличие уникального цифрового ключа (индивидуального или группового);
- низкое напряжение питания и малая потребляемая мощность;
- малые габариты и низкая цена.

Для увеличения дальности наблюдения в условиях абсолютной темноты применяется искусственная подсветка объектов при помощи инфракрасных прожекторов. В лазерных ИК-осветителях применяется импульсной режим. Объект освещается короткими импульсами лазерного излучения, и прибор включается только тогда, когда его объектива достигают отраженные от цели импульсы. В результате этого паразитные импульсы, отраженные от местных предметов, находящихся впереди и сзади объекта, а также отраженные от взвешенных в атмосфере частиц пыли, влаги, дыма не попадают в ПНВ.

Кодер

Декодер

Маскированное изображение

Демаскированное изображение

Рисунок 1.20 - Комплект маскирования видеоизображения «VideoLock»

Дальность наблюдения портативными приборами ночного видения при использовании подсветки дополнительных инфракрасных прожекторов (точечная лампа мощностью 45 Вт) достигает более 500 м.

Тепловизионные приборы, работающие в дальнем диапазоне инфракрасных волн (от 3 до 14 мкм), имеют преимущества по сравнению с ПНВ, так как их работа не зависит от уровня естественной освещенности. Кроме того, они обладают скрытностью и большой дальностью действия, способны обнаруживать замаскированные объекты. На них слабо влияют задымление и запыленность атмосферы, слепящие засветки. ТПВ способны обнаруживать следы автомашины и другой техники, способны непосредственно передавать информацию по каналам связи.

В последнее время появились тепловизоры, работающие при комнатной температуре (рис. 1.21) [83].

Рисунок 1.21 - Тепловизор ThermaCAM P640 с неохлаждаемым микроболометром и со встроенной цифровой видеокамерой

Своевременное выявление и обнаружение средств оптического наблюдения становится важной задачей при проведении как профилактических, так и специальных защитных и охранных мероприятий. Своевременное обнаружение несанкционированного наблюдения позволяет установить цель его проведения и определить потенциальную угрозу факта наблюдения.

В настоящее время наблюдается значительный рост применения подвижных видеозаписывающих систем в основном двух типов [71]:

- на основе камкодеров (видеокамеры со встроенным портативным видеомагнитофоном);
- на основе кассетных видеомагнитофонов настольного типа и миниатюрных видеокамер на приборах с зарядовой связью (ПЗС).

В системах первого типа применяются специально модифицированные компактные камкодеры с записью на 8-мм пленку или стандартную пленку для бытовых видеомагнитофонов. Камкодерные системы находят широкое применение благодаря их универсальности и меньшей стоимости технического обслуживания по сравнению с видеомагнитофонными системами. Основное их преимущество состоит в том, что их можно выносить из автомобиля для видеозаписей событий на месте преступления, или происшествия. Время записи находится в пределах от 20 мин до 2 ч, что достаточно для регистрации событий.

Классическим примером многообразия однородных форм очков ночного видения (ОНВ) можно считать модели «1ПН74» и «1ПН-94» (рис. 1.22, *а* и рис. 1.22, *б*), построенные по псевдобинокулярной схеме. Подобные приборы крепятся на

голове оператора на специальных масках для обеспечения движения и ориентирования на местности в ночное время, скрытного наблюдения объектов, выполнения различного рода инженерно-технических работ, управления транспортными средствами по пересечённой местности без использования источников видимого света в ночное время.

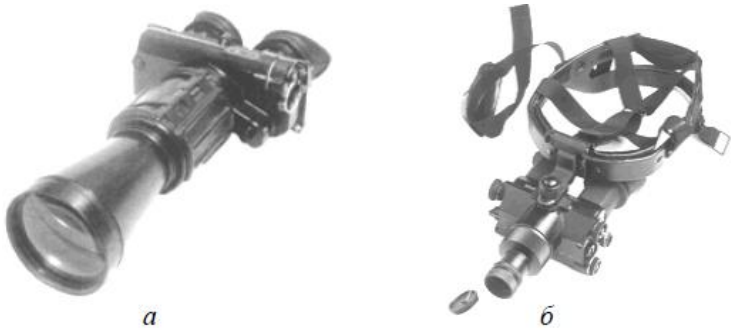


Рисунок 1.22 - Бинокль-псевдобинокуляр «1ПН-94» (*а*)
и очки ночного видения «1ПН74» (*б*)

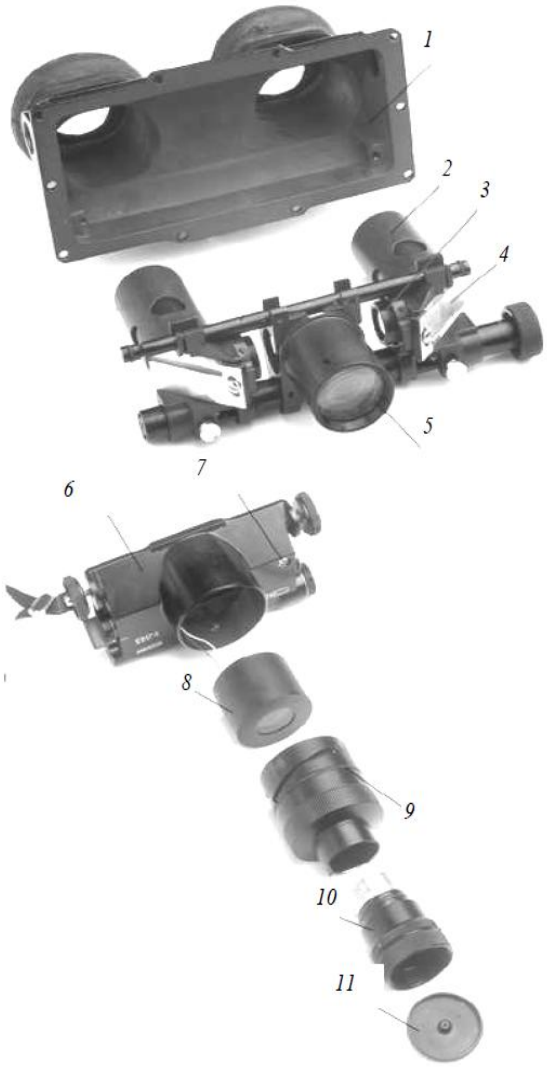


Рисунок 1.23 - Схема 1ПН74

Схема 1ПН74 показана на рис. 1.23. ОНВ содержат общий корпус *1*, окуляр *2*, оборачивающий объектив *3*, зеркало *4*, коллиматор с призмой *5*, корпус собственно ОНВ *6*, инфракрасная подсветка *7*, электронно-оптический преобразователь *8*, корпус объектива *9*, объектив *10*, крышка объектива *11*.

1.4 Средства выявления каналов утечки информации

1.4.1 Индикаторы электромагнитного поля

Принцип действия большинства индикаторов электромагнитного поля основан на широкополосном детектировании электрического поля. Индикаторы обеспечивают возможность обнаружения радиопередающих прослушивающих устройств с любыми видами модуляции [71].

Рассмотрим несколько примеров реализации индикаторов поля.

Индикатор поля-частотомер SEL SP-71M «Оберег» (рис. 1.24, *а*) является микропроцессорным индикатором поля и предназначен для мгновенного обнаружения любых источников радиоизлучения: радиомикрофонов, в том числе носимых, радиостанций, а также работающих сотовых телефонов стандарта GSM, DAMPS и DECT [81].

а *б*

Рисунок 1.24 - Индикаторы поля: *а* – частотомер «Оберег», *б* – «DP-20»

Детектор СВЧ-поля DP-20 (рис. 1.24, *б*) представляет собой электронный прибор, предназначенный для световой и звуковой индикации наличия и относительного уровня электромагнитного излучения в диапазоне частот от 900 МГц до 2,5 ГГц [71].

Индикатор позволяет обнаружить электромагнитное поле, оценить уровень сигнала и найти его источник. Возможность выбора режима акустической обратной связи (АОС) или режима звуковой индикации уровня сигнала облегчает поиск радиопередающих устройств.

Для прослушивания акустических сигналов к прибору могут быть подключены головные телефоны, при этом встроенный динамик автоматически отключается.

Десятисегментная логарифмическая светодиодная шкала и прерывистый тональный звуковой сигнал обеспечивают наглядность и удобство при работе с прибором, тональность звукового сигнала меняется в зависимости от уровня входного сигнала.

Дифференциальный детектор поля «АРК-ДДП» (рис. 1.25) разработан для обнаружения и локализации источников радиоизлучения. Выделяет сигналы микропередатчиков на фоне сильных помеховых полей. Применяется для поиска средств негласного съёма информации, использующих радиоканал в диапазоне частот от 10МГц до 3ГГц. Обнаруживает микропередатчики с любым видом модуляции и произвольной шириной спектра. Имеет малые габариты и автономное питание от встроенного аккумулятора.

Рисунок 1.25 - Индикатор поля «АРК-ДДП»

Принцип действия прибора основан на широкополосном детектировании входных сигналов. Сигнал, приходящий от источника радиоизлучения, находящегося в ближней зоне, наводит на антеннах прибора напряжения, отличающиеся по амплитуде. Эти два сигнала детектируются, вычитаются друг из друга и усиливаются. Приближение к источнику радиосигнала вызывает щелчки, частота которых пропорциональна расстоянию до источника.

Отличительная особенность прибора заключается в том, что сигналы, приходящие от удалённых радиопередатчиков, наводят на антеннах прибора одинаковые напряжения, поэтому ослабляются во много раз.

1.4.2 Сканирующие радиоприемники

В процессе контроля радиоэфира основными действиями являются поиск, обнаружение и прием требуемых радиосигналов. Возможности любого комплекса радиоконтроля, решающего эти задачи, определяются параметрами используемых

в нем сканирующих радиоприемных устройств. По сути дела именно эти устройства являются одним из важнейших функциональных элементов такого комплекса. Следует отметить, что сканирующие приемники в руках злоумышленников могут служить разведывательным средством [71].

Сканирующие радиоприемники характеризуются следующими основными показателями:

- диапазоном принимаемых частот;
- чувствительностью;
- избирательностью;
- параметрами сканирования (скоростью перестройки, полосами обзора и т.д.);
- используемым методом или методами, если они есть, обнаружения сигналов;
- видом принимаемых радиосигналов;
- оперативностью управления и возможностями его автоматизации;
- выходными параметрами (качество воспроизведения сигнала на выходе приемника, наличие выходов по промежуточной и низкой частоте, значения полос пропускания сигнала по этим частотам и т.д.);
- эксплуатационными параметрами (массогабаритные характеристики, требования по электропитанию, надежность, ремонтопригодность. удобство транспортировки и т.п.).

Представленные на отечественном рынке модели сканирующих приемников обычно удовлетворяют требованиям по диапазону и скорости сканирования для поиска радиомикрофонов или других источников радиоизлучения, не использующих режим быстрой перестройки рабочей частоты. В то же время возможность обнаружения таких радиомикрофонов или способность контроля технически сложных каналов радиосвязи зависят не только от параметров сканирования радиоприемника, но и от наличия в составе комплекса других средств, обеспечивающих решение подобных задач. В качестве таких средств в настоящее время все чаще используются специализированные комплекты программного обеспечения. В этих условиях особое значение приобретает способность сканирующего радиоприемника эффективно работать в составе автоматизированного комплекса радиоконтроля под управлением персонального компьютера. С этой целью рядом зарубежных и российских компаний производителей были разработаны так называемые «компьютерные» радиоприемники, специально ориентированные на обеспечение эффективного взаимодействия с ЭВМ. Конструктивно такие приемники выполняются либо в виде плат, встраиваемых в ISA-слот компьютера, либо в виде отдельных модулей, подключаемых к компьютеру через порты COM, LPT или PCMCIA. Благодаря такому решению обеспечивается высокая скорость обмена информацией между радиоприемником и компьютером, а отсутствие дополнительных внешних органов управления позволяет достичь небольших значений массогабаритных параметров приемника [71].

Сканирующий приемник AR5000 (рис. 1.26, *а*) предназначен для контроля радиоэфира в диапазоне частот от 10 кГц до 2,6 ГГц. Приемник обладает

высокими эксплуатационными характеристиками и большим набором сервисных функций. Приемник имеет следующие технические характеристики [71]:

- диапазон частот: 10 кГц-2600 МГц;
- виды модуляции: AM, FM, USB, LSB, CW;
- встроенный декодер DTMF и CTCSS кодов;
- полосы пропускания: 3, 6, 15, 40, 110, 220 кГц.

Сканеры японской фирмы ICOM завоевали широкое признание во всем мире. Новая модель IC-R10 (рис. 1.26, *б*) воплотила в себе все современные технологические достижения, что позволило добиться высококачественного приема сигналов всех видов модуляции в диапазоне от коротких волн до СВЧ при сохранении небольших габаритов и веса. Ряд функций впервые реализован в носимом сканере.

а *б*

Рисунок 1.26 - Сканирующие приемники «AR5000» (*а*) и «ICOM IC-R10» (*б*)

Основные характеристики сканера:

- Широкий диапазон: 0,5-1300 МГц с разрешением 100Гц.
- Виды модуляции: SSB (USB, LSB), CW, AM, FM, WFM.
- Спектроскоп. Работает в реальном времени, ширина полосы обзора ±50 или ±100кГц.
- Расширенный набор типов и видов сканирования: каждый из 2-х основных типов сканирования разбит на три вида: сплошное, диапазонное, с автоматической записью частот, по каналам памяти, по видам модуляции, по банкам памяти.
- Новая функция SIGNAVI позволяет в несколько раз увеличить реальную скорость сканирования. При сканировании в режиме FM используется дополнительный приемный контур, который продолжает сканирование при нахождении основным приемником сигнала, таким образом, основной приемник сканирует «скачками» только по занятым каналам. Величина скачков составляет до 5 шагов настройки, но не более 100 кГц.

1.4.3 Анализаторы спектра, радиочастотомеры

Кроме сканирующих приемников для радиотехнической разведки могут применяться и ряд других устройств таких как анализаторы спектра, радиочастотомеры, интерсепторы, селективные микро вольтметры [71].

Характерной особенностью большинства таких устройств являются их портативное исполнение и высокая чувствительность как следствие достижений в области радиоэлектроники.

Анализаторы спектра позволяют анализировать спектр принятых сигналов в заданном диапазоне частот.

Радиотестеры измеряют параметры сигналов, работают со всеми типами модуляции.

Радиочастотомеры предназначены для измерения частоты источника радиосигнала.

Для перехвата разговоров, ведущихся по каналам радиосвязи в ближней зоне, могут использоваться интерсепторы. Интерсептор автоматически настраивается на частоту наиболее мощного сигнала и осуществляет его детектирование.

Примеры технической реализации некоторых перечисленных устройств приведены ниже.

Входные усилители перекрывают диапазон от 10 Гц до 3000 МГц а максимальная точность измерения составляет 1 Гц. Такие характеристики позволяют применять 3000A Plus практически в любых областях радиотехники, где необходимо быстро и с высокой точностью проводить измерения частот.

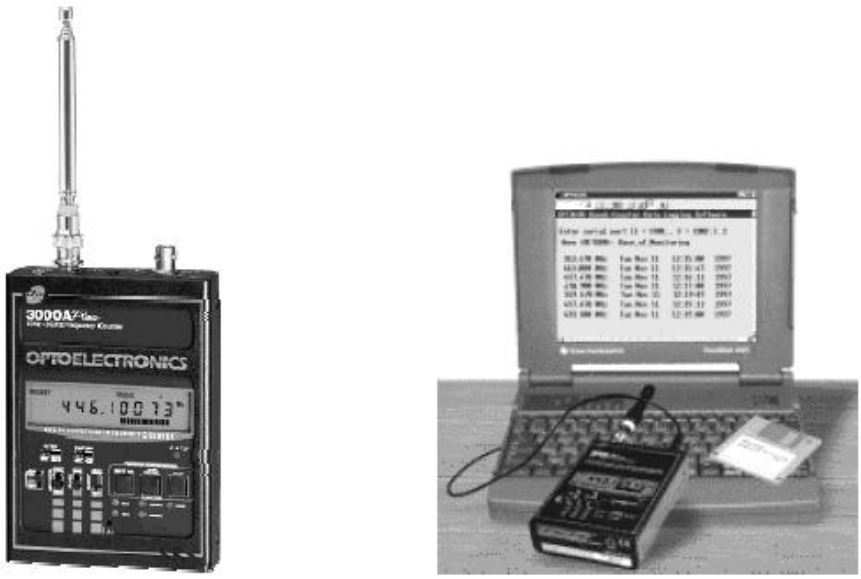


Рисунок 1.27 - Портативный многофункциональный частотомер «3000A Plus»

Для достижения максимальной чувствительности, частотомер имеет три входных усилителя и два входа для подключения антенн. Измеряться могут как частоты источников радиоизлучения, так и частоты в электрических схемах при контактном подключении с помощью щупов. При контактных подключениях

измеряться могут не только частоты но и временные характеристики сигналов (в том числе и длительность одиночных импульсов). В этом случае используются усилители с входным сопротивлением 1 МОм.

Усилители с входным сопротивлением 1 МОм позволяют использовать 3000A Plus для измерения частот и временных характеристик сигналов в электронных схемах. Измеряться могут как периодические, так и импульсные сигналы напряжением до 50 вольт [81].

Анализатор спектра HP8591E (рис. 1.28, *а*) предназначен для проведения специальных исследований электронно-вычислительной техники и слаботочного оборудования на наличие и уровень побочных электромагнитных излучений и наводок; для контроля радиоэлектронной обстановки в проверяемых помещениях с возможностью накопления информации об объекте и сравнительного анализа с уже имеющимися, полученными ранее, данными; для проверки эффективности принимаемых мер по защите информации при проведении пуско-наладочных работ и функционировании технических средств обработки информации. Имеется возможность управления работой анализатора с использованием ПЭВМ и СПО [81].

а *б*

Рисунок 1.28 - Анализаторы спектра «HP8591E HP» (*а*) и «ESA-L1500A» (*б*)

Анализатор спектра HP ESA-L1500A (рис. 1.28, *б*) предназначен для проведения специальных исследований электронно-вычислительной техники и слаботочного оборудования на наличие и уровень побочных электромагнитных излучений и наводок; для контроля радиоэлектронной обстановки в проверяемых помещениях с возможностью накопления информации об объекте и сравнительного анализа с уже имеющимися, полученными ранее, данными; для инженерных исследований изымаемых органами МВД технических средств (радиостанций, радиомикрофонов, систем съема информации и т.д.); для проверки эффективности принимаемых мер по защите информации при проведении пуско-наладочных работ и функционировании технических средств обработки информации. Имеется возможность управления работой анализатора с использованием ПЭВМ и СПО. Диапазон рабочих частот – 9…1,5 ГГц [81].

1.4.4 Многофункциональные комплекты для выявления каналов утечки информации

Портативный комплект для обнаружения средств съема информации и выявления каналов ее утечки «ПКУ-6М»

Портативный комплект для обнаружения средств съема информации и выявления каналов ее утечки «ПКУ-6М» представляет собой удобную в работе многофункциональную поисковую систему (рис. 1.29).

Рисунок 1.29 - Портативный комплект для обнаружения средств съема информации и выявления каналов ее утечки «ПКУ-6М»

Система предназначена для выявления [84]:

- средств съема информации с передачей сигнала по существующим проводным коммуникациям;
- утечки речевой информации по акустическому и вибро-акустическому каналам;
- средств съема информации с передачей сигнала по оптическому каналу.

Система содержит комплект датчиков, позволяющих:

- выявить каналы утечки акустической информации через сквозные щели и трещины ограждающих конструкций;
- оценить вибро-акустические свойства ограждающих конструкций и инженерных коммуникаций;

- обнаружить электрические сигналы в слаботочных линиях в полосе частот 0,3…10 кГц;

- обнаружить электрические сигналы в сильноточных линиях в полосе частот 0,03…24, 5 МГц;

- выявить оптическое излучение осветительных приборов, индикаторов, датчиков сигнализации, блоков дистанционного управления в видимом и инфракрасном диапазонах.

В состав комплекта «ПКУ-6М» входят:

- основной блок-анализатор;
- микрофон со звукопроводом;
- вибро-электрический датчик;
- оптический датчик;
- имитатор многофункциональный «ИМФ-2»;
- головные телефоны;
- комплект соединительных кабелей;
- комплект съемных зажимов и щупов;
- сетевой адаптер питания.

Поисковая система «ПКУ-6М» обеспечивает:

- обнаружение сигналов низкой частоты в полосе 0,3…10 кГц;

- прием сигналов с амплитудной (АМ) и частотной (ЧМ) модуляцией в диапазоне частот 30…24500 кГц;

- автоматическую перестройку в рабочем диапазоне частот;

- визуальное отображение спектров принимаемых сигналов на ЖК-дисплее;

- прослушивание принимаемого сигнала при помощи встроенного динамика или головных телефонов;

- запись аудио- сигнала в режимах RF (индикация уровня сигнала в мВ) и AF (индикация уровня выходного сигнала усилителя низкой частоты в дБ) на внутренний носитель.

В режиме SP спектроанализатора сканирование по установленному диапазону частот можно проводить как в ручном, так и в автоматическом режимах. Скорость автоматического режима работы составляет примерно 10 кГц/с с дискретностью 1 кГц.

В режиме панорамы PN на экране дисплея после сканирования одновременно может отображаться полоса частот шириной не более 1440 кГц.

После остановки автоматического сканирования в режиме PN можно выбрать одно из действий:

- продолжить сканирование в ручном режиме;

- установить курсор настройки центральной частоты просмотра на выбранный участок панорамы;

- перейти в режим просмотра спектра в диапазоне ±25 кГц от текущей центральной частоты;

- возобновить получение панорамы от текущего значения центральной частоты.

Изменение вида модуляции при прослушивании детектированных сигналов производится нажатием соответствующей кнопки.

Осциллографический просмотр низкочастотных сигналов возможен как в режиме AF, так и в режиме RF. В режиме RF осциллограмма AM или FM сигнала приводится после детектора. При переходе в режим AF на экране автоматически появляется осциллограмма низкочастотного входного сигнала анализатора.

Кроме контроля с помощью встроенного громкоговорителя или головных телефонов выявленный аудиосигнал может быть записан на встроенное устройство. Запись осуществляется схемой электронной памяти прибора, состоящей из нескольких банков. Выбор банков памяти при записи осуществляется автоматически.

Устройство позволяет выполнить последовательную запись нескольких сигналов, которые могут быть прослушаны в ходе последующего анализа. Объем памяти позволяет записывать сигналы продолжительностью до 16 мин.

При заполнении памяти прибор продолжает запись аудиосигнала, последовательно стирая предыдущую информацию.

Имеющийся в составе системы многофункциональный имитатор «ИМФ-2» предназначен для имитации работы средств съема информации при проведении поисковых мероприятий и как источник тестирующих сигналов.

Рассмотрим особенности выявления каналов утечки информации.

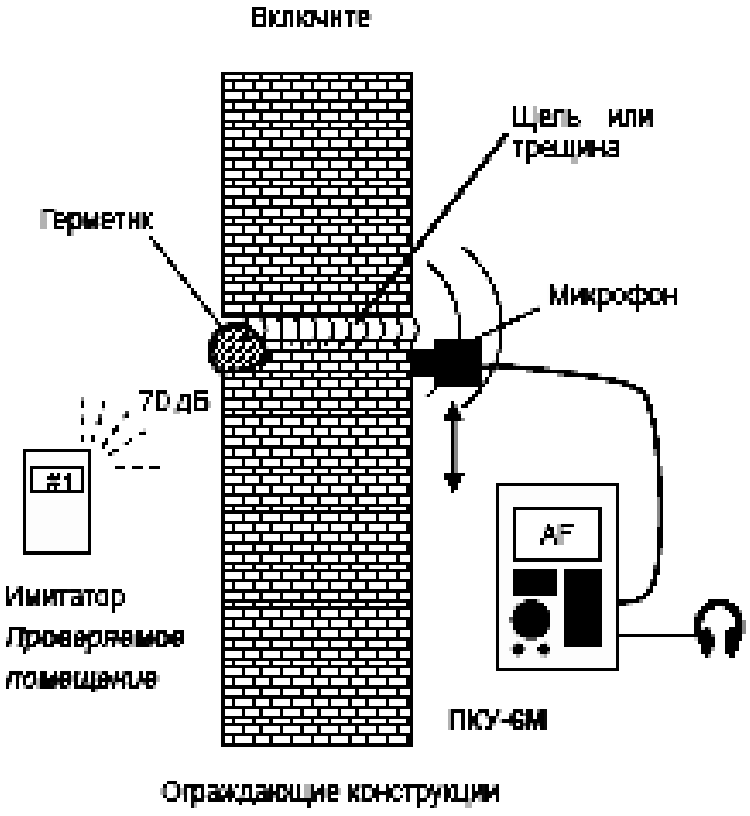


Рисунок 1.30 - Схема исследования акустического канала

Акустический канал

При визуальном обследовании помещения отмечаются возможные каналы прямой воздушной проводимости – окна, щели, трещины, вентиляциионные

каналы. Исследование предполагаемого акустического канала утечки информации проводится по схеме рис. 1.30.

Имитатор в режиме «AUDIO» создает со стороны проверяемого помещения тестовый акустический сигнал с уровнем 70 дБ. Уровень прошедшего через ограждение сигнала измеряется микрофоном и основным блоком, работающим в режиме AF, и характеризует звукопоглощающие свойства ограждающей конструкции.

Если организовать озвучивание помещения речевым сигналом, то через наушники можно оценить его разборчивость.

Подобные действия необходимо провести во всех подозрительных местах и выявить места наилучшего прохождения акустического сигнала.

Виброакустический канал

При визуальном обследовании помещения отмечаются все жесткие конструкции (балки, колонны, бетонные стены, трубы и т.п.), выходящие за пределы контролируемой зоны. Исследование предполагаемого виброакустического канала утечки информации проводится по схеме рис. 1.31.

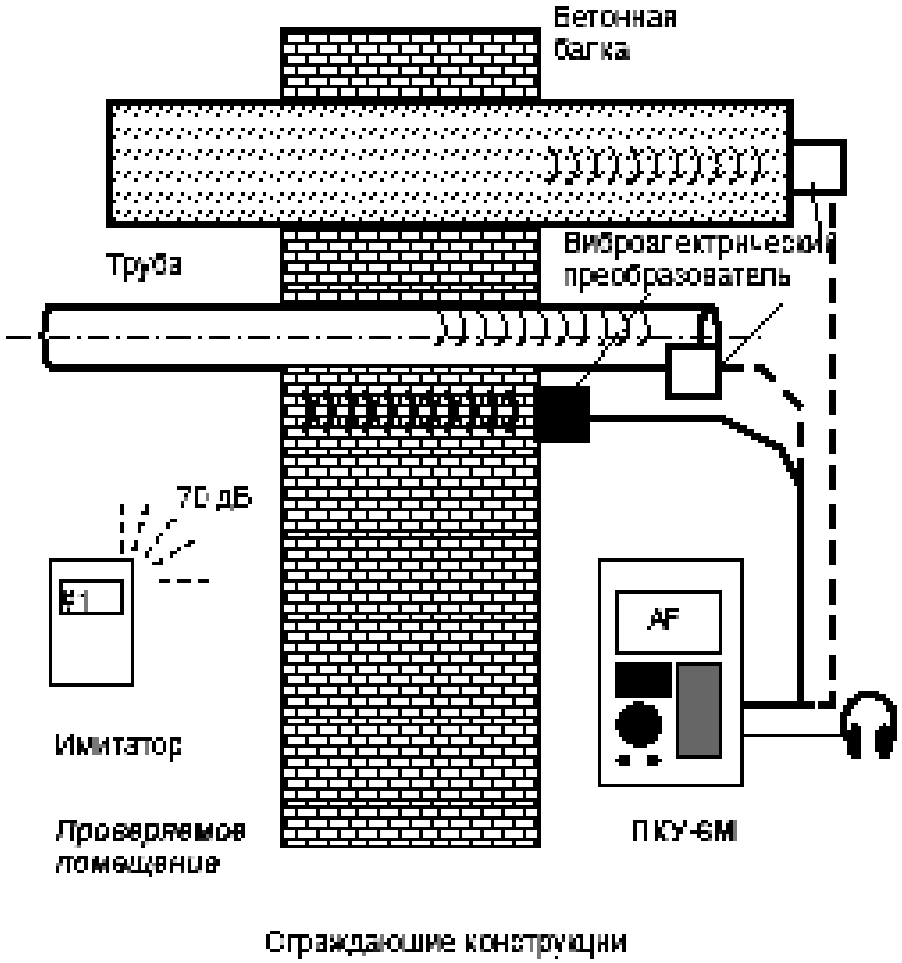


Рисунок 1.31 - Схема исследования виброакустических каналов

Схема исследования виброакустических каналов такая же как и схема исследования акустических каналов, только микрофон заменяется

виброакустическим датчиком, который должен иметь плотный контакт с жесткой конструкцией с усилием порядка 5 кГ.

Имитатор в режиме «AUDIO» создает со стороны проверяемого помещения тестовый акустический сигнал с уровнем 70 дБ. Уровень прошедшего через ограждение сигнала измеряется виброакустическим датчиком и основным блоком, работающим в режиме AF.

Выявление микрофонного эффекта и обнаружение скрытых микрофонов

Перед началом поисковых работ необходимо изучить все проводные коммуникации, выходящие за пределы контролируемой зоны, и провести исследования по схеме рис. 1.32.

Наличие микрофонного эффекта осуществляется следующим образом. Имитатор переводится в режим работы «AUDIO» и последовательно устанавливается на расстоянии 1 м от офисного оборудования. Основной блок подключается через входной комплектный низковольтный кабель к проверяемой проводной линии. Наличие микрофонного эффекта оценивается по появлению сигналов в головных телефонах.

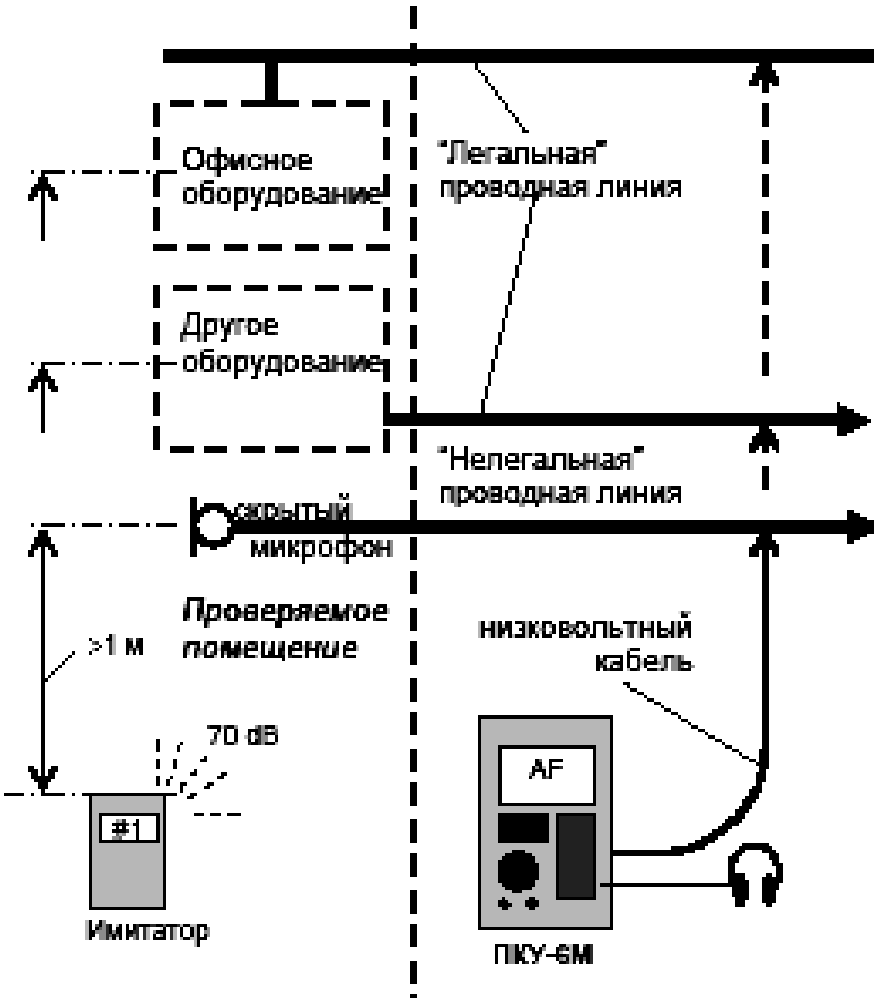


Рисунок 1.32 - Выявление микрофонного эффекта и обнаружение скрытых микрофонов

Офисное оборудование исследуется при всех режимах его работы.

Для выявления скрытно установленных в ограждающих конструкциях основной блок подключается к проводной линии неизвестного назначения. В линию от основного блока подается постоянное напряжение 15В с поочередной сменой полярности и включается имитатор. Наличие микрофона оценивается по характерному сигналу в головных телефонах.

Проверка электрических сигналов в сетях электропитания и слаботочных линиях

Этот вид проверки производится по схеме рис. 1.33 и подробных пояснений не требует.

Входной сетевой кабель подключается к проверяемой линии и входному блоку. Поочередно в режимах FM и AM модуляции производится поиск сигналов в линиях.

В режиме анализа спектра производится поиск скрытых микрофонов в линиях. При обнаружении сигнала от скрытно установленного микрофона обследуется проверяемая линия последовательным подключением к различным ее участкам с целью определения максимального уровня принимаемого сигнала. Место нахождения микрофона определяется при включенном встроенном громкоговорителе, используя явление «акустической завязки».

Проверка слаботочных линий

Проверка слаботочных линий осуществляется по схеме рис. 1.33. В этом режиме работы входной сетевой кабель заменяется на низковольтный кабель или кабель с 6-ти или 8-ми контактными адаптерами (рис. 1.34) [71].

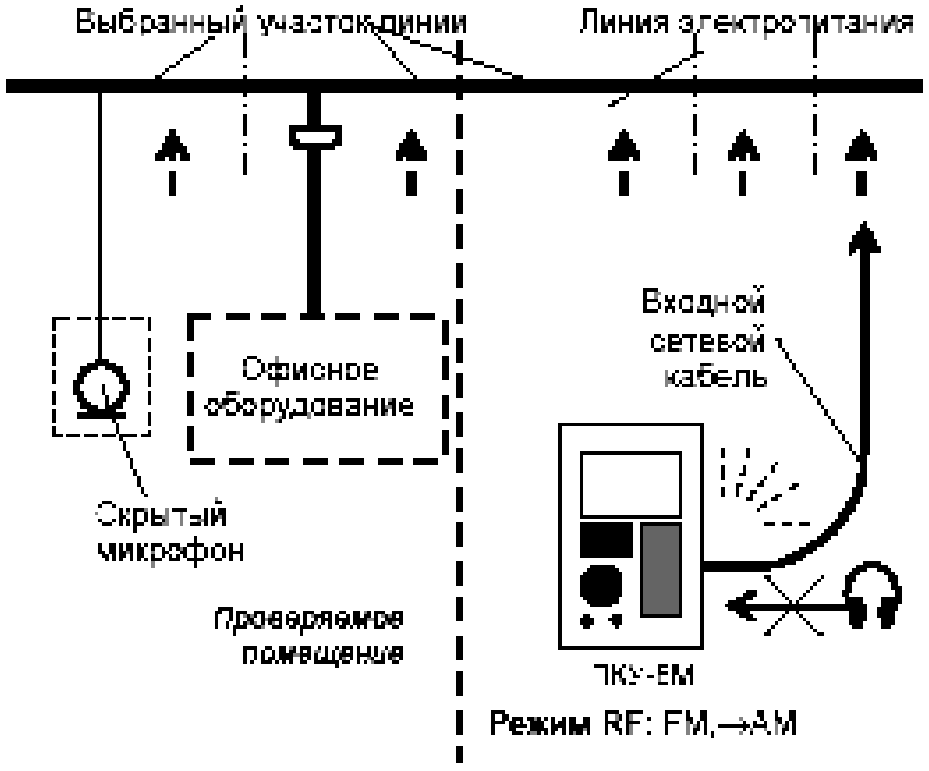


Рисунок 1.33 - Проверка электрических сигналов в сетях электропитания и линиях

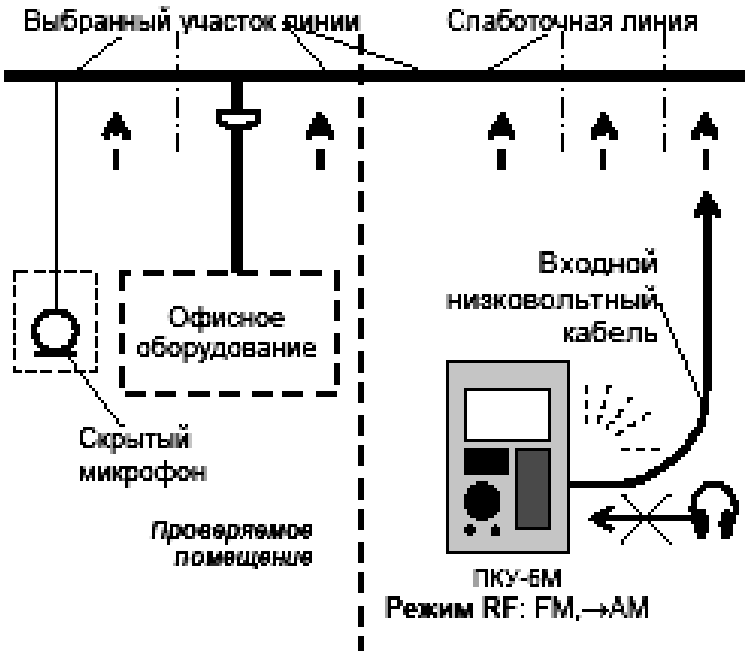


Рисунок 1.34 - Проверка слаботочных линий

Проверка оптического канала

Проверка оптического канала осуществляется по схеме рис. 1.35.

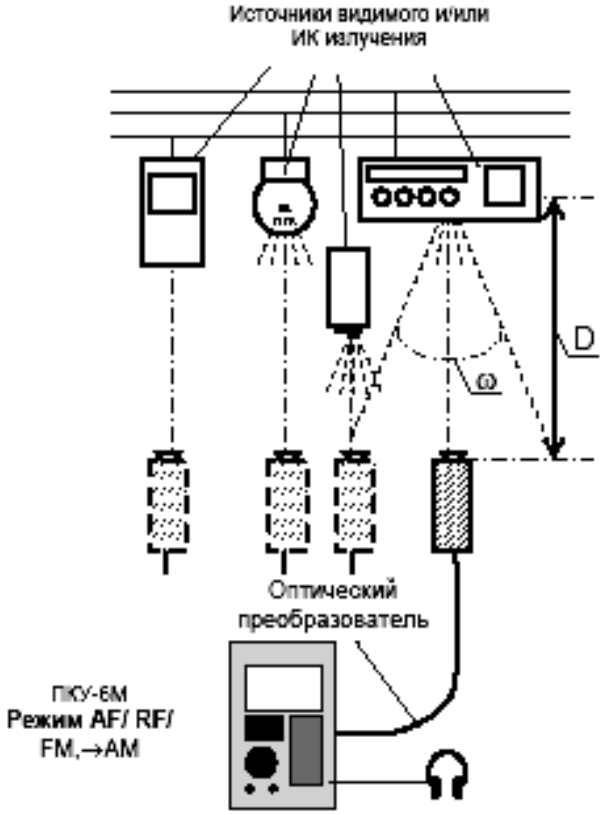


Рисунок 1.35 - Проверка оптического канала

Перед проверкой определяются источники видимого и инфракрасного излучения, которые могут стать причиной утечки информации по оптическому каналу:

- осветительные приборы;
- датчики охранной сигнализации;
- пульты дистанционного управления;
- световые индикаторы электронной аппаратуры.

Имитатор помещается в месте проведения переговоров и совещаний и переводится в режим работы «AUDIO» (озвучивание). На основном блоке устанавливается режим AF и к нему подключаются оптический датчик и головные телефоны. Оптический преобразователь направляется в сторону обследуемых объектов и определяется наличие в головных телефонах характерного тона, соответствующего сигналу имитатора. Удаляя оптический преобразователь от проверяемого оборудования, определяется направление и расстояние, на котором прием сигналов еще имеет место. Указанные операции повторяются в режиме RF [71].

1.4.5 Портативный комплект для обнаружения средств съема информации и выявления каналов ее утечки «Пиранья»

Близким по назначению к «ПКУ-6М» является комплект ST 031 «Пиранья». Он предназначен для проведения оперативных мероприятий по обнаружению и локализации технических средств негласного получения информации, а также для выявления и контроля естественных и искусственно созданных каналов утечки информации (рис. 1.36) [85].

Рисунок 1.36 - Комплект ST 031 «Пиранья»

Прибор состоит из основного блока управления и индикации, комплекта преобразователей и позволяет работать в следующих режимах:

- высокочастотный детекторчастомер;
- сканирущий анализатор проводных линий;
- детектор ИК-излучений;
- детектор низкочастотных магнитных полей;
- дифференциальный низкочастотный усилитель;
- виброакустический приемник;
- акустический приемник.

Переход прибора в любой из режимов осуществляется автоматически при подключении соответствующего преобразователя. Информация отображается на графическом ЖКИ дисплее с подсветкой, акустический контроль осуществляется через специальные головные телефоны, либо через встроенный громкоговоритель. Управление прибором производится с помощью 16-ти кнопочной клавиатуры. Обеспечивает возможность запоминания в энергозависимой памяти 99-ти изображений [71].

Прибор позволяет обрабатывать поступающие низкочастотные сигналы в режиме «осциллограф» либо «спектроанализатор» с индикацией численных параметров. В ST 031 «Пиранья» предусмотрен вывод на дисплей контекстной помощи в зависимости от режима работы. Возможен выбор как русского, так и английского языка.

ST 031 «Пиранья» выполнен в носимом варианте. Для его переноски и хранения используется специальная сумка, приспособленная для компактной и удобной укладки всех элементов комплекта. Предварительный этап подготовительных мероприятий предстоящей контрольно-поисковой работы состоит в заблаговременном детальном изучении объекта. При этом изучаются условия расположения объекта, а также его конструктивные особенности. Кроме того, важное значение на этом этапе имеют оформление интерьера помещения (состав и размещение мебели) и оснащенность техническими средствами (ПЭВМ, ксероксы, факсы, телефонные аппараты, бытовая техника и т. п.). Считается целесообразным полученные данные в произвольной форме протоколировать. На этом этапе следует также выявить наличие и расположение проводных и других потенциально опасных коммуникаций.

1. Использование прибора для выявления каналов утечки информации в радиочастотном диапазоне

Эти каналы могут быть созданы как преднамеренно за счет использования заинтересованными органами и организациями специальных технических средств съема информации, так и возникнуть естественным образом за счет побочных электромагнитных излучений технических средств обработки информации. В любом случае возникает необходимость классификации сигналов в радиочастотном диапазоне по совокупности критериев.

1.1. Один из практических подходов к классификации радиосигналов

С точки зрения решения задач контроля защиты информации с использованием прибора «Пиранья», все радиосигналы, попадающие в его

рабочий диапазон, можно достаточно обоснованно разделить на «опасные» и «неопасные» [71].

«Опасные» радиосигналы могут быть созданы как внутренними, так и внешними источниками. На практике встречается довольно большое число их самых разнообразных сочетаний.

Обычно к числу чисто «внутренних опасных» радиосигналов относят:

- сигналы «радиозакладок» (радиомикрофоны, телефонные радиотрансляторы и т.п.).
- сигналы радиомаяков;
- сигналы несанкционированно включенных в помещении радиостанций и радиотелефонов;
- побочные электромагнитные излучения ПЭВМ и других технических средств обработки информации.

К категории «опасных» в сочетании «внутренние-внешние» принято относить радиосигналы, источниками которых могут быть:

- радиомикрофоны с выносным акустическим микрофоном;
- телефонные радиоретрансляторы, установленные на линии связи за пределами помещения (но вблизи него);
- радиостетоскопы, установленные с наружной стороны ограждающих помещение поверхностей;
- вынесенные передатчики скрытых видеокамер;
- устройства внешнего высокочастотного облучения.

1.2. Методы поиска и локализации источников опасных радиосигналов

В случае обнаружения потенциально опасного радиосигнала следует двигаться в направлении возрастания его уровня. Контроль за уровнем принимаемого сигнала необходимо осуществлять по показаниям индикаторов уровня на экране дисплея прибора и по частоте щелчков звуковой сигнализации в режиме «TONE».

Метод акустической завязки основан на возникновении положительной акустической обратной связи между микрофоном «радиозакладки» и динамиком прибора «Пиранья». При этом обязательно включение звуковой сигнализации прибора в режиме «AUD» для вывода на динамик демодулированного сигнала. Эффект акустической завязки возникает только в отношении радиозакладки, в которой применены обычные виды модуляции – амплитудная и частотная (узкополосная или широкополосная) [71].

Признаком возникновения акустозавязки является появление характерного «писка», тон и интенсивность которого изменяются при приближении динамика прибора к микрофону радиозакладки.

Эффективность выбора того или другого метода во многом зависит от особенностей, присущих потенциально опасным радиосигналам и их источникам.

1.3. Особенности потенциально опасных радиосигналов и их источников

Радиомикрофоны. Широкое распространение имеют радиомикрофоны с параметрической стабилизацией частоты передатчика. Основная их особенность – большие пределы девиации несущей частоты (до нескольких мегагерц). Поэтому

для локализации радиомикрофонов такого типа наиболее целесообразно использование метода «акустозавязки» [85].

В качестве высокопрофессиональных средств негласного добывания информации применяются радиомикрофоны с вынесенным передатчиком. Их основная особенность – разнос мест установки микрофона и собственно радиопередатчика (вплоть до выноса в другое помещение). В этом случае необходимо сочетание метода «акустозавязки» и амплитудного метода. При этом для локализации микрофона необходимо использовать метод «акустозавязки», а радиопередатчика (в проверяемом помещении или за его пределами) – амплитудный метод.

Высокопрофессиональными средствами являются и радиомикрофоны с закрытым или маскированным радиоканалом. Их основная особенность состоит в том, что принятый и демодулированный сигнал не несет в себе информации об акустическом фоне помещения. Это определяется использованием для закрытия (маскирования) радиоканала методов инверсии спектра, цифровых методов передачи и сложных видов модуляции. Поэтому в основе их обнаружения и локализации должен лежать амплитудный метод с дополнением его анализом осциллограмм и спектрограмм.

Другие источники потенциально опасных радиоизлучений [85]. К ним относятся радиостетоскопы, скрытые видеокамеры с радиоканалом передачи информации, радиозакладки в ПЭВМ, радиомаяки, средства пространственного высокочастотного облучения, несанкционированно включенные средства связи (радиостанции, радиотелефоны, телефоны с радиоудлинителями).

Для создания акустического фона и для активизации радиозакладок с акустопуском следует подготовить и разместить в контролируемом помещении тестовый источник звука.

Если не имеется ограничений на скрытность проведения работ, то наилучший эффект дает сочетание амплитудного метода и метода акустозавязки. При проведении скрытного поиска необходимо применять амплитудный метод с прослушиванием детектированных сигналов через головные телефоны.

Особое внимание при работе следует обратить на радиоизлучения в диапазоне 60–640МГц, наиболее типичном для использования радиомикрофонами и телефонными радиоретрансляторами. Поиск осуществляется путем последовательного обхода помещения (объекта) с движением вдоль стен и обследованием мебели и других предметов. При отсутствии ограничений на использование метода акустозавязки динамик встроенного громкоговорителя прибора следует ориентировать в сторону обследуемых поверхностей и предметов.

При приближении антенны прибора «Пиранья» к месту размещения радиозакладки напряженность электромагнитного поля возрастает и повышается уровень сигнала на его входе.

При достаточном приближении к источнику радиочастотомер осуществляет захват частоты и показывает в строке экрана ее значение по результатам нескольких измерений. Путем уменьшения громкости, изменения границ динамического диапазона, увеличения вручную порога срабатывания детектора,

постоянного наблюдения за показаниями частотомера сужается зона обследования и, тем самым, локализуется место установки радиозакладки с погрешностью в пределах 10–15 см [71].

В случае применения в качестве радиозакладки телефонов стандарта DECT или GSM, помимо индикации повышения уровня сигнала в нижней строке, на индикаторе появится надпись DECT или GSM.

Аналогично поиску радиомикрофонов осуществляется поиск телефонных радиоретрансляторов. При этом для их активизации необходимо снять трубки всех телефонных аппаратов. Поиск проводится в два этапа. Сначала проверяются на наличие закладных устройств сами телефонные аппараты. Установленный в аппарате радиоретранслятор проявляется точно так же как и радиомикрофон. Далее поиск телефонных радиоретрансляторов осуществляется путем обхода помещения вдоль абонентской телефонной линии и выявления на ней мест с максимальным уровнем радиосигнала. При обходе антенну прибора необходимо ориентировать в разных плоскостях на минимально возможном расстоянии от линии. Практически всегда существует необходимость проверки линии вплоть до основного распределительного щита.

Поиск радиостетоскопов имеет определённые особенности, обусловленные способами их применения (установка вне контролируемого помещения). Поэтому для обнаружения сигналов радиостетоскопов необходимо обследовать все доступные внешние поверхности ограждающих конструкций.

Поскольку средой распространения виброакустических колебаний могут являться трубы отопления и водоснабжения, то проверке подлежат и эти коммуникации.

Принципиально передатчики видеокамер могут работать на частотах до 2300 МГц. Обнаружение сигнала (похожего на сигнал яркости) на частотах вне диапазона телевизионного вещания практически однозначно свидетельствует о работе передатчика скрытой видеокамеры. Локализация таких средств осуществляется амплитудным методом.

Применительно к пространственному высокочастотному облучению основной является задача выявления факта создания этого искусственного канала добывания информации. Обычно она решается в два этапа [85]. На первом этапе выявляется факт облучения помещения высокочастотным сигналом. На втором этапе отслеживается отклик на зондирующий высокочастотный сигнал. При этом необходимо ориентироваться на следующие факторы. Остронаправленный луч электромагнитной энергии может быть сформирован только на очень высоких частотах (800–900 МГц и выше). Радиоволны этого диапазона распространяются в условиях прямой видимости между источником излучения и облучаемыми предметами, поэтому в качестве основных путей их проникновения в контролируемое помещение определяют прежде всего оконные проемы. Переизлучающими объектами могут быть обычные для данного помещения технические средства, обладающие так называемым микрофонным эффектом. К ним обычно относят динамики бытовых громкоговорителей, акустические системы даже выключенной аудиоаппаратуры, телефонные аппараты с электрическим звонком и т.п. Переизлученный на частотах высших (чаще всего

второй или третьей) гармоник сигнал локализуется в непосредственной близости от облучаемых предметов и имеет модуляцию акустическим фоном помещения.

Исходя из этого, может быть определен следующий порядок работы. Для выявления факта высокочастотного облучения поочередно провести обследование потенциально опасных оконных проемов. По графическому индикатору оценить стабильность частоты излучения. Перейти в любое из соседних помещений (ориентированных окнами в ту же сторону) и повторить проверку в районе каждого из его оконных проемов.

Высокочастотное облучение вполне вероятно, если:

- частота принимаемого сигнала лежит (или очень близка) в пределах указанного диапазона;
- стабильность частоты высокая;
- модуляция сигнала отсутствует.

2. Использование прибора для выявления каналов утечки информации по проводным линиям различного назначения

Рассмотрим приёмы выявления искусственно созданных каналов утечки информации по проводным линиям на основе использования специальных технических средств. Основными видами проводных линий, для анализа которых предназначен прибор «Пиранья», являются линии электросети (высокопотенциальные линии), а также абонентские телефонные линии и линии систем пожарной и охранной сигнализации (низкопотенциальные линии) [85].

В целом приёмы и методы, применяемые для проверки проводных линий названных видов, одинаковы. Подключение к ним осуществляется с использованием универсального адаптера. Анализу методом сканирования подвергается общий диапазон от 0 до 15МГц. Вывод результатов сканирования производится в виде изображения панорамы с однотипным представлением измеренных параметров. Функции органов управления прибором одинаковы (вне зависимости от вида проверяемой линии).

3. Использование прибора для выявления каналов утечки информации в инфракрасном диапазоне

Принципиально следует рассматривать два вида таких каналов утечки информации. Один из них создается за счет применения специальных технических средств с передачей перехваченной информации в инфракрасном диапазоне. Другой канал основан на облучении стекол оконных проемов направленным лучом источника инфракрасных излучений и приеме отраженного сигнала, промодулированного речевым сигналом [85].

Для выявления обоих каналов утечки необходимо провести одинаковые подготовительные мероприятия. Прежде всего следует правильно выбрать время проведения проверки, а именно такое, когда в окна контролируемого помещения не попадают прямые солнечные лучи. В самом помещении необходимо выключить лампы накаливания и источники интенсивного теплового излучения. Специфика инфракрасных закладок предполагает необходимость обеспечения прямой видимости между передатчиком закладки и приемником инфракрасных излучений. Поэтому в помещении путь прохождения излучения передатчика наружу может проходить только через оконные проемы. С учетом этих

особенностей, поиск опасных сигналов следует начинать от окон помещения, передвигаясь вглубь его. Признаком наличия инфракрасного излучения является появление окрашенных сегментов шкалы индикатора уровня и щелчков звуковой индикации в режиме «TONE». Анализ обнаруженных сигналов может производиться на слух в режиме «AUD», а также визуально с использованием встроенных осциллографа и анализатора спектра. Локализация источников инфракрасного излучения наиболее точно осуществляется сочетанием амплитудного метода и метода акустозавязки. При этом порядок действий такой же как и при работе в режиме высокочастотного детектора-частотомера.

4. Использование прибора для выявления каналов утечки информации по низкочастотным магнитным полям

Для таких каналов характерно то, что они возникают при использовании по целевому назначению санкционированных средств (ПЭВМ, переговорных устройств, систем звукоусиления, магнитофонов, телефонов и т.д.). Поэтому одной из основных задач следует считать исследование таких средств на наличие, интенсивность и дальность низкочастотного магнитного поля. Сопутствующими могут считаться задачи поиска скрытой (несанкционированно проложенной) проводки и обнаружения работающих диктофонов [85].

Перед проведением работ целесообразно выключить в помещении люминесцентные светильники, а антенну прибора, при необходимости, включить в дифференциальном режиме (переключатель на корпусе антенны поставить в положение «к белой точке»).

Потенциальные источники опасных низкочастотных магнитных полей следует проверять раздельно, включая их в работу поочередно.

При исследовании технических средств необходимо оценить дальность распространения магнитных полей и особенности их спектра. Для этого первоначально необходимо разместить магнитную антенну в непосредственной близости от исследуемого объекта и зафиксировать по осциллограмме относительный уровень поля. Удаляясь от исследуемого средства и изменяя пространственную ориентацию антенны, оценить дальность уверенного приема низкочастотного сигнала.

Применительно к усилителям звуковой частоты, имеющим выходной трансформатор, следует оценить дальность уверенного (разборчивого) приёма речевого (тестового) сигнала.

Такая оценка может послужить основой для правильного выбора мест установки соответствующих средств по отношению к наружной стороне помещения и варианта их совместного расположения в помещении. При необходимости включить режим «SA», проанализировать спектрограмму и записать ее в энергонезависимую память.

Для поиска скрытой проводки необходимо последовательно обойти все стены помещения, располагая магнитную антенну в непосредственной близости к ним. Зафиксировать область возрастания уровня поля и путем перемещения антенны по горизонтали и вертикали определить прохождение трассы скрытой проводки.

5. Использование прибора для оценки эффективности виброакустической защиты и звукоизоляции помещений

Оценка эффективности виброакустической защиты помещения обычно проводится в два этапа. На первом этапе защита, если она имеется, должна быть выключена и произведена проверка собственно виброакустических свойств ограждающих помещение поверхностей. Для этого необходимо виброакустический датчик прикреплять в различных местах проверяемых поверхностей (стен, дверей, окон, по возможности пола и потолка) с внешней, по отношению к контролируемому помещению, стороны. Включить источник тестового звукового сигнала. Он может размещаться либо в обычном месте ведения конфиденциальных разговоров, либо на определённом расстоянии *L* от обследуемой поверхности [85].

Уровень звука обычно устанавливают соответствующим громкой речи (74 дБ). Для калиброванных источников звука расстояние «*L*» выбирают в пределах 1,0…2,0 м. Сначала на качественном уровне (путём прямого прослушивания) оцениваются виброакустические свойства обследуемых поверхностей, а затем, переходом в режим «SA», количественно оцениваются амплитуды частотных составляющих тестового сигнала.

На втором этапе, если это предусмотрено, оценивается эффективность системы виброакустической защиты. Для этого на каждой поверхности как качественно на слух, так и количественно по спектрограмме определяется соотношения уровней тестового и маскирующего сигнала, а также выявляются «не прикрытые» составляющие спектра. Это служит объективной основой коррекции амплитудно-частотной характеристики источников маскирующего сигнала.

Согласно общепринятым правилам разборчивость речевых сигналов гарантированно не восстанавливается, если маскирующий шум (помеха) в 4–5 раз (16 дБ) превышает их уровень. Полное исключение признаков речи достигается при 8-ми кратном превышении уровня сигнала помехой, создаваемой системой активной защиты.

Оценку звукоизоляции помещений также целесообразно проводить в два этапа. На первом этапе, используя тестовый источник сигнала с уровнем звука, соответствующим громкой речи, установить соответствие между этим уровнем и показаниями прибора в режимах осциллографа и анализатора спектра. Для этого необходимо разместить акустический излучатель источника звука и микрофон прибора на некотором фиксированном расстоянии. Обычно его выбирают в пределах 1,0…2,0 м [85].

На втором этапе оцениваются звукоизоляционные свойства ограждающих конструкций, эффективность системы активной защиты (зашумления), а также возможность утечки речевой акустической информации через элементы вентиляции, различного рода ниши, сквозные отверстия и т.п.

Для оценки звукоизоляционных свойств ограждающих конструкций тестовый источник звука может быть расположен либо в обычном месте ведения конфиденциальных разговоров, либо на расстоянии от обследуемой поверхности.

Размещением микрофона в различных местах смежных (выше и ниже расположенных) помещений качественно на слух и количественно по спектрограмме определяется дальность перехвата речевого сигнала из данного помещения и оценка снижения уровня звукового сигнала за счёт свойств ограждающих поверхностей, а также наличие наименее ослабленных составляющих спектра. Последнее даёт возможность принять обоснованное решение о необходимости дополнительной защиты, в том числе и активной, и выбор характеристик средств защиты.

Поскольку воздуховоды систем вентиляции являются наиболее опасными каналами утечки речевой акустической информации, то они подлежат обязательной проверке. Для этого микрофон прибора необходимо ввести в выходное (входное) отверстие воздуховода каждого из смежных помещений. Качественно на слух оценивается прохождение и разборчивость сигнала от тестового источника, а по показаниям прибора в режиме осциллографа или анализатора спектра – его ослабление при прохождении по воздуховоду до места размещения микрофона. Правильная оценка ослабления может быть получена только в том случае, если имеется детальная схема системы вентиляции [85].

1.4.6 Многофункциональный комплекс радиомониторинга и выявления каналов утечки информации «АРК-Д1ТИ»

Комплекс (рис. 1.37) позволяет проведение специальных исследований технических средств на сверхнормативные побочные электромагнитные излучения и наводки (ПЭМИН), радиомониторинг, поиск технических каналов утечки информации, технический анализ, специальные функции [81].

АРК-Д1ТИ – многофункциональный портативный комплекс третьего поколения для выявления технических каналов утечки информации и радиомониторинга.

Рисунок 1.37 - Комплекс «АРК-Д1ТИ»

Комплекс решает задачи:

- оценка защищенности основных технических средств и систем, предназначенных для обработки, хранения и передачи по линиям связи конфиденциальной информации;
- оценка защищенности конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счет наводок на вспомогательные технические средства, системы и их коммуникации;
- оценка защищенности речевой конфиденциальной информации от утечки за счет акустоэлектрических преобразований во вспомогательных технических средствах и системах;
- контроль в реальном масштабе времени радиоэлектронной обстановки в районе защищаемых объектов военного и государственного назначения в пределах контролируемой зоны, выявление различного рода нарушений, связанных с несанкционированным включением излучающих средств, находящихся на территории защищаемых объектов, и контроль эффективности работы средств защиты.

В состав комплекса входят:

- центральный модуль АРК-Д1ТИ в кейсе;
- широкополосная измерительная антенна АРК-А7И;
- широкополосная антенна АРК-А2М (комплект из трех антенн);
- широкополосная наружная антенна АРК-А5;
- пакет программ СМО-ДХИ;
- IBM совместимая ПЭВМ.

1.4.7 Комплекс RS turbo

Комплекс RS turbo (рис. 1.38) выполняет все функции комплекса RS turbo Mobile-L, однако позволяет сканировать радиодиапазон вплоть до 12 ГГц с дополнительным конвертером. С помощью конвертера RS/L комплекс обнаруживает сигналы, которые передаются подслушивающими устройствами по сети электропитания или любым проводным линиям в диапазоне от 0,6 кГц до 10 МГц, а также в инфракрасной части оптического диапазона [86].

В частности, для анализа проводных и оптических каналов используется конвертер RS/L, а для нейтрализации выявленных источников радиоизлучений – программируемый генератор RS/N (до 1800 МГц). С помощью антенного коммутатора RS/K комплекс может контролировать радиообстановку с помощью нескольких антенн, предназначенных для различных диапазонов или установленных в пространственно разнесенных помещениях. Контроллеры акустических систем RS/Z используются для обнаружения и определения местоположения радиомикрофонов методом акустического зондирования в удаленных помещениях.

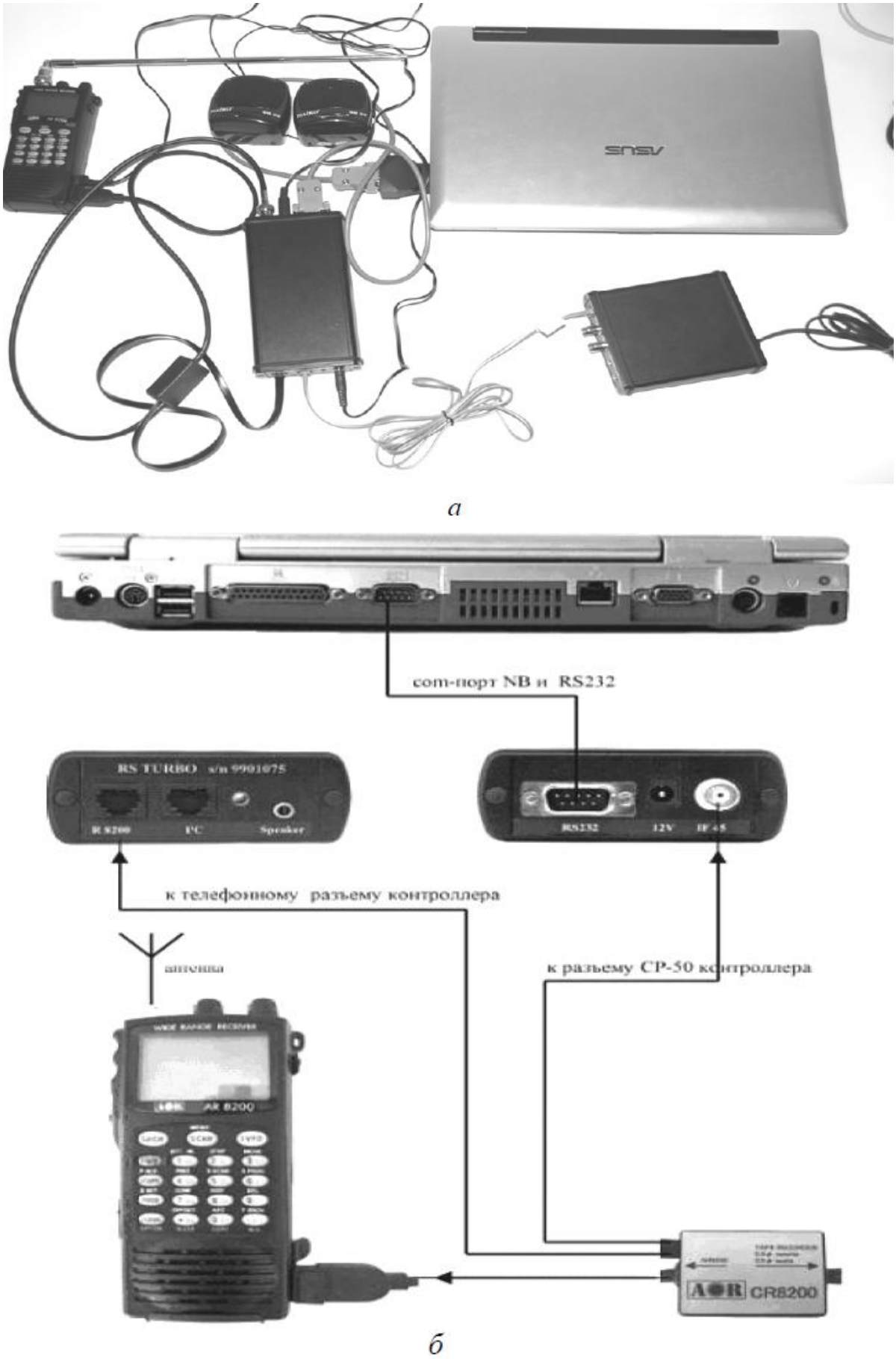


Рисунок 1.38 - Комплекс RS turbo: *а* – общий вид, *б* – схема включения

Общая схема соединений аппаратуры комплекса RS turbo: компьютера, сканирующего радиоприемника, местной акустической системы и контроллера показана на рис. 1.38, *б*. На лицевой стороне корпуса контроллера RS turbo находятся светодиод, индицирующий наличие напряжения питания, которое поступает от собственного блока питания, телефонный разъём для подключения к последовательному порту управления приемником, телефонный разъём шины I2C для подключения дополнительных периферийных устройств, а также гнездо для подключения акустических колонок «Speaker». На задней стороне контроллера находятся разъём для подключения последовательного интерфейса RS232 компьютера (COM-порт), гнездо круглого разъема питания 12 вольт и разъём CP-50 для подключения выхода промежуточной частоты приемника AR8200.

К контроллеру поставляется комплект специальных соединительных кабелей, различных для каждого типа приемников.

Сканирование

Сканирование – это базовая операция, которая предшествует обнаружению, классификации и идентификации источников излучений (сигналов). В процессе сканирования выявляются занятые участки исследуемого частотного диапазона и оцениваются спектры присутствующих в нем сигналов. Частота настройки сканирующего приемника изменяется дискретно с фиксированным шагом 8 МГц и на каждом шаге вычисляемый контроллером RS turbo результат измерений уровней принимаемых во всем спектре сигналов заносится в компьютер. В анализаторе RS turbo быстрое сканирование выполняется с широким (200 кГц) или узким (12,5 кГц) шагом. По результатам сканирования компьютер формирует спектральную панораму исследуемого диапазона, в которой каждому значению частоты настройки соответствует измеренный спектр сигнала. Операции сканирования выполняются в порядке их размещения в списке операций задания. Это дает возможность в первую очередь просматривать те участки спектра, где вероятность найти излучения несанкционированных источников выше. Один частотный диапазон можно включать в задание несколько раз, чтобы реализовать различные алгоритмы идентификации и классификации излучений [86].

Выполнив один цикл сканирования, программа составляет таблицу, в которой каждому значению частоты настройки ставится в соответствие измеренный последовательным анализатором контроллера RS turbo спектр сигналов в полосе анализа 8 МГц, снятый для сигналов, превышающих заданный порог, с разрешением 12,5 кГц. Эта таблица называется спектральной панорамой. Программа комплекса RS turbo позволяет формировать спектральные панорамы с учетом данных, полученных в ходе текущего и любого числа предшествующих циклов сканирования. После выполнения первого цикла сканирования таблица спектральной панорамы сохраняется в памяти компьютера. На следующем цикле формируется новая (текущая) таблица, а значения уровней в таблице предыдущей панорамы модифицируются в соответствии с выбранным методом обработки:

- обновление (в таблицу записывается новое значение, а старое стирается);
- накопление (в таблицу записывается больший из двух уровней);
- усреднение (в таблицу записывается среднее двух уровней).

Первый из перечисленных методов обычно используется в процессе обнаружения излучений, а следующие два – для сбора данных, характеризующих обстановку в заданных диапазонах при продолжительных наблюдениях со статистической обработкой результатов измерений. Накопление максимальных значений обеспечивает наиболее полный учет всех излучений, появлявшихся за время наблюдения. Накопление средних значений позволяет при большом числе циклов сканирования свести к нулю уровни случайных сигналов, например, импульсных помех. Текущая панорама отображается на экране зеленым цветом и показывает уровни, измеренные в текущем цикле сканирования.

Данные, полученные в результате обработки уровней предшествующих циклов сканирования, отображаются красным цветом и располагаются на заднем плане. В любой момент после остановки сканирования таблица панорамы, отражающая результаты выполненных циклов сканирования, может быть сохранена в виде файла (файл панорамы спектра, расширение .pan) с заданным программой или пользователем именем. Спектральные панорамы, характеризующие обстановку в заданном диапазоне частот, называются диаграммами загрузки диапазона. Такие панорамы на экране отображаются синим цветом и используются в качестве фона для обнаружения «неизвестных» излучений [86].

При необходимости данные, отражающие результаты предшествующих циклов сканирования, могут быть удалены из списка командой очистки. При этом в исходную таблицу панорамы записываются нулевые уровни. Если программа работает с несколькими заданиями, то таблица уровней составляется и модифицируется для каждого из них. При этом на экране отображаются панорамы спектров активного задания. В процессе анализа проводных линий с помощью конвертора RS/L plus текущий спектр зеленого цвета выводится на экран на фоне спектра красного цвета, полученного на предыдущем цикле.

Для повышения скорости работы комплекс RS turbo выполняет сканирование с помощью последовательного анализатора спектра с разрешением 12,5 КГц с шагом 8 МГц. После запуска сканирование ведется с указанным шагом по сетке частот. Начальная и конечная частоты указанного в задании диапазона заменяются ближайшими частотами этой сетки. На каждом шаге контроллер RS turbo измеряет уровни принимаемых сигналов, т.е. снимает спектр на широкополосном выходе промежуточной частоты приемника, и передает данные в компьютер.

Обнаружение

Обнаружение – базовая операция выявления всех радиоизлучений (сигналов), уровень которых в заданном диапазоне превосходит установленное в задании пороговое значение (порог обнаружения). В процессе обнаружения программа оценивает параметры сигнала: ширину спектра, максимальный уровень, несущую частоту, а также классифицирует обнаруженные излучения, распределяя их по группам в соответствии с определенными признаками. Обнаруженные излучения автоматически классифицируются программой RS turbo по следующим признакам:

- «известные» и «неизвестные»;

- «обнаруженные ранее» и «вновь появившиеся»;
- «стандартные» и «нестандартные».

Анализ

Операции анализа необходимы для выявления среди множества обнаруженных сигналов «опасных» излучений, которые могут быть созданы передатчиками подслушивающих устройств. Идентификация (опознавание) сигналов подслушивающих устройств в программе RS turbo выполняется автоматически или в ручном режиме с помощью следующих операций [86]:

- анализ гармонического состава излучений;
- корреляционный анализ откликов на акустические импульсы;
- спектральный анализ;
- временной и спектральный анализ сигналов на выходе демодулятора.

Кроме того, в процессе анализа откликов на импульсы акустического зондирования программа измеряет расстояния от колонок акустической системы комплекса до микрофона и определяет местоположение микрофона в помещении (локализация источника излучения).

1.4.8 Комплексы измерения ПЭМИН

Программно-аппаратный комплекс «СИГУРД» (рис. 1.39) представляет собой одну из самых совершенных систем оценки защищенности технических средств по каналу ПЭМИН и предназначен для проведения специальных исследований различных технических средств по выявлению, распознаванию и измерению сигналов их побочных электромагнитных излучений с максимальной степенью автоматизации процедур [87].

Рисунок 1.39 - Программно-аппаратный комплекс «СИГУРД»

Система создана на базе анализатора спектра фирмы IFR (MARCONI) или других производителей, стандартного IBM-совместимого персонального компьютера (настольного или Notebook) и комплекта антенн. Могут быть применены любые антенны, предназначенные для работы в диапазоне от 9 кГц до 2 ГГц. Рекомендуется применение активных широкополосных антенн. Антенный коэффициент вводится в управляющую программу и учитывается автоматически при выборе соответствующей антенны. Замена антенн в процессе измерений осуществляется оператором в соответствии с сообщениями управляющей программы.

Основным отличием данной системы от аналогичных разработок является четырёхэтапное обнаружение и измерение сигналов и полностью автоматическое, адаптивное распознавание частот (сигналов) ПЭМИН и автоматическое дистанционное управление параметрами тест-режимов на исследуемой ПЭВМ (на базе типового IrDA канала).

На первом этапе выполнения задания в автоматическом режиме осуществляется фильтрация всех входных сигналов по энергетическому критерию (превышение на заданную величину над уровнем шумов). Далее система выполняет коррекцию каждого выявленного сигнала, уточняя его частоту. На третьем этапе осуществляется корреляционный двухступенчатый анализ сигналов в сравнении их с эталоном, хранящимися в файловой библиотеке. Эталон сигнала синтезируется оператором по спектрограмме реального сигнала в процессе формирования задания. Предусмотрено выделение сигналов, корреляционные характеристики которых не позволяют программе сделать однозначный вывод, и выдача их на экран оператору для принятия решения. На последнем этапе выполняется измерение выявленных «опасных» сигналов [87].

Все спектры, зафиксированные в процессе специальных исследований, могут быть сохранены для последующего анализа. Данная функция позволяет дополнительно вести анализ спектров методом «наложения», при котором сравниваются два спектра, снятых в разных режимах работы исследуемого устройства. Изменения спектра по сравнению с сохранённым при наложении выделяются цветом.

Управляющая программа позволяет управлять всеми необходимыми режимами работы анализатора спектра. Все задаваемые оператором параметры запоминаются в виде «задания». Библиотека заданий сохраняется для последующего использования, в том числе любое задание может быть использовано в последующем без изменений или с любыми изменениями. Выполнение любого задания может быть приостановлено оператором в любой момент и продолжено или запущено сначала или продолжено с изменёнными в случае необходимости параметрами.

Предусмотрен и ручной режим работы с анализатором спектра при управлении всеми его функциями от компьютера. Анализатором спектра можно управлять и автономно с помощью его органов управления. При этом при возврате под управление компьютера оператор может продолжить выполнение задания с параметрами, предусмотренными заданием или с введёнными с пульта управления анализатора спектра вручную.

Задача расчёта требуемых параметров исследуемых устройств решается отдельным программным модулем, использующим результаты измерений ПЭМИН исследуемого устройства в виде файла данных и дополнительные данные, вводимые оператором. Итогом расчёта является таблица данных измерений и расчётов, предназначенная для включения в отчёт.

Анализатор спектра может работать непрерывно от автономного источника электропитания до полутора часов, что позволяет в ряде случаев минимизировать уровень помех при измерениях. Рекомендуемые измерительные антенны также предусматривают автономное электропитание. Таким образом, при использовании компьютера «Notebook», весь комплекс может быть мобильным и автономным.

Программно-аппаратный комплекс «ЛЕГЕНДА» (рис. 1.40) предназначен для автоматизированного контроля побочных электромагнитных излучений и наводок, а также выявления и контроля акустоэлектрических преобразований в исследуемых технических средствах [82].

Рисунок 1.40 - Программно-аппаратный комплекс «ЛЕГЕНДА»

Комплекс «Легенда» создан на базе современных приборов ведущих производителей радиоизмерительной аппаратуры: «Agilent Technologies», «Rohde Schwarz», «Tektronix», «Advantest» и др.

В состав комплекса входят:

- радиоизмерительный прибор (обычно анализатор спектра фирмы «Agilente Technologies» E4411B, 9 кГц – 1,5 ГГц) с опциями;

- антенный коммутатор;

- система измерительная «Альбатрос» (9 кГц – 1 ГГц);

- эквивалент сети EMCO 3810/2;

- управляющая ЭВМ (обычно NoteBook) с интерфейсом GP-IB (National Instruments) и GP-IB кабелями;

- комплект для обнаружения акустоэлектрических преобразований;

- специальное программное обеспечение: управляющая программа, расчетные программы, комплект тестов для ПЭВМ (под WIN 95/98).

Отличительные особенности комплекса:

- два этапа обнаружения ПЭМИН исследуемых технических средств в автоматизированном режиме (устранение «чужих сигналов»):

- выделение пика на фоне шумов («энергетический» критерий);

- распознавание образа сигнала (сравнение эталонного сигнала с сигналом приемного устройства в текущий момент);

- достоверность и повторяемость результатов измерений;

- возможность применения различных антенных систем в том числе и старого парка аппаратуры (RFT);

- возможность полуавтоматического обнаружения и измерения сигналов, измерения по сформированным шаблонам (наибольшая скорость проведения исследований);

- автоматическое формирование протоколов измерений;

- использование самых распространенных текстовых редакторов – «Microsoft Office», «Word Pad» и «Note Pad» при оформлении отчетных документов.

Для обнаружения и измерения уровней сигналов создается образ эталонного сигнала с помощью специального редактора эталонов. Определяется программа проведения исследований.

По команде оператора комплекс сканирует указанный в настройках диапазон, обнаруживает и измеряет сигналы ПЭМИН ПЭВМ.

Имеется возможность прерывать работу для подключения или изменения характеристик антенн. Измеренные значения заносятся в таблицу, которая затем может сохраняться в виде файла на диске.

Переносной комплекс для проведения инженерных исследований и исследований на сверхнормативные побочные электромагнитные излучения «НАВИГАТОР-П6-Г» (Е4407В) представлен на рис. 1.41. Он предназначен для автоматического, автоматизированного и экспертного поиска сигналов ПЭМИН от проверяемых технических средств, измерения частоты и пикового значения амплитуды найденных сигналов, хранения, обработки и представления результатов поиска и измерений в удобном для оператора виде, и применяется на объектах сферы обороны и безопасности [82].

Применяемое специальное программное обеспечение (СПО) позволяет максимально автоматизировать процессы измерений, обработки их результатов, выполнения необходимых расчетов и подготовки отчетной документации по результатам выполненных исследований.

Рисунок 1.41 - Переносной комплекс «НАВИГАТОР-П6-Г»

В программно-аппаратном комплексе реализованы четыре метода поиска ПЭМИН:

- метод сравнения панорам;
- аудио-визуальный метод;
- экспертный метод;
- параметрически-корреляционный метод.

Первые три метода позволяют осуществлять поиск ПЭМИН в автоматизированном режиме. Четвертый метод обеспечивает полностью автоматический поиск и выявление информативных ПЭМИН.

В состав комплекса входят измерительная и управляющая подсистемы. Связь между подсистемами осуществляется с помощью интерфейсов RS-232 или GPIB. С помощью измерительной подсистемы комплекса проводятся измерения электрической и магнитной составляющих электромагнитного поля, а также наводок в проводных коммуникациях. Параметры измеренных сигналов передаются из измерительной подсистемы в управляющую, где происходит их обработка, представление на экране в удобном для оператора виде и хранение в виде файлов.

Программно-аппаратный комплекс позволяет [82]:

- в автоматическом и автоматизированном режимах 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 в соответствии с утвержденными методиками;

- проводить инженерные исследования специальных технических средств (радиостанций, радиомикрофонов, систем съема информации и т.д.).

1.4.9 Комплекс для измерения характеристик акустических сигналов СПРУТ-7

Комплекс СПРУТ-7 (рис. 1.42) обеспечивает проведение исследований характеристик и проверку эффективности систем акустического и виброакустического зашумления помещений, измерение уровней электрического и магнитного полей и наводок на проводные коммуникации, проведение статистической обработки результатов измерений [88].

Комплекс может использоваться при измерении и гигиенической оценке шумов и вибрации в жилых и производственных помещениях на соответствие санитарным нормам.

Специальное программное обеспечение комплекса СПРУТ-7 не требует от пользователя каких-либо особых навыков работы на ПЭВМ, кроме знания общих правил работы в среде WINDOWS.

Основные элементы комплекса имеют автономное питание, что делает его мобильным и удобным в эксплуатации.

Подключение модуля сопряжения к ПЭВМ и его питание осуществляется по шине USB.

В программно-аппаратный комплекс «Спрут-7» входят:

1) Измерительная подсистема на базе анализатора шума и вибраций 1-го класса точности SVAN в составе:

- измерительный модуль с октавным анализом, третьоктавным анализом и функцией БПФ;
- измерительный микрофон;
- измерительный акселерометр;
- измерительные щупы;
- измерительная пассивная антенна EMCO-6511 с рабочим диапазоном частот 0,2–5000 кГц либо аналогичная;
- адаптер – усилитель для подключения измерительных щупов и антенн; стойка для установки измерительного модуля;
- зарядное устройство.

Рисунок 1.42 - ПАК «Спрут-7»

2) Подсистема источника тестового акустического сигнала в составе:

- модуль источника тестового акустического сигнала;
- экранированная акустическая система, используемая при проведении измерений акустоэлектрических преобразований;
- стойка для установки акустической системы;
- зарядное устройство.

3) Подсистема управления:

- модуль сопряжения с ПК;
- ПЭВМ типа «ноутбук»;
- специальное программное обеспечение.

4) Комплект оборудования для обеспечения автономного электропитания объектов ВТСС.

Специальное программное обеспечение позволяет работать с комплексом как с измерительным прибором, а также проводить измерения и обрабатывать результаты в соответствии с методикой ФСТЭК.

1.5 Скрытие и защита информации от утечки по техническим каналам

1.5.1 Концепция и методы инженерно-технической защиты информации

Системы технической защиты

Концепция инженерно-технической защиты информации определяет основные принципы, методы и средства обеспечения информационной безопасности объектов. Она представляет собой общий замысел и принципы обеспечения информационной безопасности объекта в условиях угроз и включает в себя [71]:

- оценку угроз;
- систему защиты информации;
- принцип построения системы защиты информации.

Инженерно-техническая защита представляет собой совокупность специальных органов, технических средств и мероприятий по их использованию для защиты конфиденциальной информации.

Эффективная техническая защита информационных ресурсов является неотъемлемой частью комплексной системы обеспечения информационной безопасности и способствует оптимизации финансовых затрат на организацию защиты информации. Техническая защита информации предполагает комплекс мероприятий по защите информации от несанкционированного доступа по различным каналам, а также нейтрализацию специальных воздействий на нее – уничтожения, искажения или блокирования доступа.

Цели и задачи технической защиты [71]:

- предотвращение проникновения злоумышленника к источникам информации с целью уничтожения, хищения или изменения;
- защита носителей информации от уничтожения в результате различных природных и техногенных воздействий;
- предотвращение утечки информации по различным техническим каналам.

Принципы проектирования систем технической защиты [72]:

- непрерывность защиты информации в пространстве и во времени, постоянная готовность и высокая степень эффективности по ликвидации угроз информационной безопасности;
- многозональность и многорубежность защиты, задающее размещение информации различной ценности во вложенных зонах с контролируемым уровнем безопасности;
- избирательность, заключающаяся в предотвращении угроз в первую очередь для наиболее важной информации;
- интеграция (взаимодействие) различных систем защиты информации с целью повышения эффективности многокомпонентной системы безопасности;
- создание централизованной службы безопасности в интегрированных системах.

По функциональному назначению средства инженерно-технической защиты подразделяются на следующие группы [72]:

- инженерные средства, представляющие собой различные устройства и сооружения, противодействующие физическому проникновению злоумышленников на объекты защиты;

- аппаратные средства (измерительные приборы, устройства, программно-аппаратные комплексы и др.), предназначенные для выявления каналов утечки информации, оценки их характеристик и защиты информации;

- программные средства, программные комплексы и системы защиты информации в информационных системах различного назначения и в основных средствах обработки данных;

- криптографические средства, специальные математические и алгоритмические средства защиты компьютерной информации, передаваемой по открытым системам передачи данных и сетям связи.

В концепции инженерно-технической защиты информации кроме целей и задач системы безопасности, определяются принципы ее организации и функционирования; правовые основы; виды угроз и ресурсы, подлежащие защите, а также основные направления разработки системы безопасности, включая: физическую, правовую, организационную, экономическую, инженерно-техническую, программно-математическую защиту, информационно-аналитическое обеспечение и консультативную помощь [71].

К целям защиты информации относятся: предотвращение утечки, хищения, утраты, искажения, подделки информации и предотвращение других несанкционированных негативных воздействий.

Безопасная информационная деятельность требует наличия системы ее защиты – комплекса организационных, организационно-технических и технических мероприятий по обнаружению, предотвращению и ликвидации возникших угроз объекту.

Создание новой системы защиты или оценка эффективности существующей системы безопасности объекта начинается с анализа возможных угроз и оценки их реального появления. Основой для анализа является исследование объекта на наличие уязвимостей в защите, изучение расположения и особенностей инженерных конструкций, коммуникаций и т.п. На следующем этапе осуществляется выбор соответствующих методов и средств адекватной защиты.

При оценке вероятных угроз объекту должны учитываться угрозы здоровью и безопасности персонала; угрозы целости и сохранности материальных ценностей и оборудования; безопасность информации, сохранность государственной или коммерческой тайны.

Для получения максимально реальной оценки угроз необходимы изучение и анализ статистических данных, связанных с попытками разведывательной деятельности на объекте в прошлом; оценка риска по каждому виду угроз; оценка ситуации на объекте и прилегающих к нему территориях на определенном интервале времени; изучение статистики по фактам разведдеятельности на подобных объектах.

Важным моментом в объективной оценке угроз и в разработке концепции защиты объекта является привлечение независимых экспертных организаций или специализированных государственных учреждений, имеющих

квалифицированный персонал. В этом случае исключается субъективная оценка разведдоступности объекта и проводится квалифицированная разработка концепции защиты.

Несмотря на большое разнообразие возможных информационных угроз, проектирование защиты от каждой из них должно вписываться в комплексную систему защиты. Комплексная система защиты предусматривает надежное перекрытие всех опасных каналов утечки информации.

Эффективность системы защиты основных и вспомогательных технических средств от утечки информации по техническим каналам оценивается по различным критериям, которые определяются физической природой информационного сигнала, но чаще всего по соотношению «сигнал/шум».

Все способы защиты согласно руководящей документации делятся на две группы [71]:

- скрытие;
- дезинформация.

К первой группе относятся:

- пассивное скрытие;
- активное скрытие;
- специальная защита.

Ко второй группе относятся:

- техническая дезинформация;
- имитация;
- легендирование.

Суть пассивного скрытия заключается в исключении или значительном затруднении обнаружения объектов, а также в ослаблении до необходимого уровня их демаскирующих признаков.

Пассивное скрытие состоит из организационных мероприятий и технических мер.

К организационным мероприятиям относятся [71]:

- территориальное, пространственно-временное, энергетическое и частотное ограничения на функционирование объектов;
- затруднения для ведения технической разведки путем использования маскирующих свойств местности, местных предметов, времени суток;
- установление контролируемых зон в месте расположения скрываемых видовых объектов.

К техническим мерам пассивного скрытия относятся [71]:

- снижение контрастности демаскирующих признаков скрываемых видовых объектов по отношению к фону;
- снижение уровня информационных физических полей, создаваемых функционирующим объектом;
- применение маскирующих покрытий для видовых объектов;
- камуфлирование техники;
- применение при настройке радиоэлектронной аппаратуры эквивалентов антенн, закрытых антенно-фидерных устройств, экранированных камер и

сооружений, исключающих электромагнитные излучения в окружающее пространство.

Суть активного скрытия состоит главным образом в создании маскирующих шумовых помех различной физической природы техническим средствам разведки и в создании ложной обстановки по физическим полям скрываемого объекта [71].

Активное скрытие применяется в большинстве случаев как дополнительная мера к пассивному скрытию, когда не обеспечиваются условия снижения уровня физического поля до безопасного значения.

Спецзащита реализуется аппаратными, криптографическими и программными способами. К спецзащите относятся скремблирование телефонных переговоров, кодирование цифровой информации криптографическими методами, программные методы модификации информации.

К принципам инженерно-технической защиты информации относятся [71]:

- надежность защиты информации;
- непрерывность защиты;
- скрытность защиты информации;
- рациональность защиты;
- многообразие способов защиты;
- комплексное применение различных способов и средств защиты;
- экономичность защиты.

1.5.2 Экранирование электромагнитных волн

Для снижения наводок необходимо устранять или ослаблять до допустимых значений паразитные связи. В первую очередь ослабление паразитных связей должно производиться прямым уменьшением паразитной емкости, взаимной индуктивности и паразитного сопротивления. Способы уменьшения паразитных связей в принципе несложны: размещение вероятных источников и приемников наводок на максимально возможном расстоянии друг от друга; уменьшение габаритов токонесущих элементов, обеспечивающих минимум паразитной связи (для получения минимальной взаимоиндуктивности катушек индуктивности их оси должны быть взаимно перпендикулярны); сведение к минимуму общих сопротивлений; изъятие посторонних проводов, проходящих через несколько узлов или блоков, которые могут связать элементы, расположенные достаточно далеко друг от друга; при невозможности исключения посторонних проводов, создающих паразитную связь, необходимо позаботиться о том, чтобы при емкостной паразитной связи сопротивление постороннего провода относительно корпуса было минимальным, при индуктивной паразитной связи необходимо увеличивать внутреннее сопротивление посторонней линии связи, последнюю очередь – экранирование и развязывающие фильтры [71].

Экранирование – это локализация электромагнитной энергии в пределах определенного пространства путем преграждения ее распространения.

Развязывающий фильтр – это устройство, ограничивающее распространение помехи по проводам, являющимся общими для источника и приемника наводки.

Введение экранов часто требует существенного изменения компоновки, конструкции, а иногда и габаритов изделия, поэтому конструктор должен ясно понимать физическое действие каждой детали экрана, влияние любого элемента конструкции на значения паразитных связей. Желательно совмещать элементы экранов с элементами несущей конструкции. Общая рекомендация сводится к тому, что на начальном этапе конструирования необходимо принимать все возможные меры для снижения паразитных связей, а уж потом в ходе экспериментальной доводки изделия убрать те элементы, которые оказались лишними. Исключить какой-либо элемент из готового изделия почти всегда проще, чем добавить.

Экранирование электромагнитных волн является основой экологической безопасности и одним из самых действенных средств защиты объекта от утечки информации по техническим каналам [71].

В связи с бурно развивающейся техникой все острее становится проблема формирования электромагнитной обстановки, обеспечивающей нормальное функционирование электронных устройств и экологическую безопасность. Электромагнитная обстановка представляет собой совокупность электромагнитных полей в заданной области пространства, которая может влиять на функционирование конкретного радиоэлектронного устройства или биологического объекта.

Для создания благоприятной электромагнитной обстановки и для обеспечения требований по электромагнитной безопасности объекта, которая включает в себя и противодействие несанкционированному доступу к информации с использованием специальных технических средств, производится экранирование электромагнитных волн.

Применение качественных экранов позволяет решать многие задачи, среди которых защита информации в помещениях и технических каналах, задачи электромагнитной совместимости оборудования и приборов при их совместном использовании, задачи защиты персонала от повышенного уровня электромагнитных полей и обеспечение благоприятной экологической обстановки вокруг работающих электроустановок и СВЧ-устройств.

Под экранированием в общем случае понимается как защита приборов от воздействия внешних полей, так и локализация излучения каких-либо средств, препятствующая проявлению этих излучений в окружающей среде. В любом случае эффективность экранирования – это степень ослабления составляющих поля (электрической или магнитной), определяемая как отношение действующих значений напряженности полей в данной точке пространства при отсутствии и наличии экрана, Так как отношение этих величин достигает больших значений, то удобнее пользоваться логарифмическим представлением эффективности экранирования [71]:

$$K_E = 201g\frac{E_0}{E_1}, dB,$$
$$K_H = 201g\frac{H_0}{H_1}, dB, \qquad (1.2)$$

где K_E – коэффициент ослабления (экранирования) по электрической составляющей,

K_H – коэффициент ослабления (экранирования) по магнитной составляющей,

E_0 (H_0) – напряженность электрической (магнитной) составляющей поля в отсутствии экрана,

E_1(H_1) – напряженность электрической (магнитной) составляющей поля при наличии экрана в той же точке пространства.

Теоретическое решение задачи экранирования, определение значений напряженности полей в общем случае чрезвычайно затруднительно, поэтому в зависимости от типа решаемой задачи представляется удобным рассматривать отдельные виды экранирования: электрическое, магнитостатическое и электромагнитное. Последнее является наиболее общим и часто применяемым, так как в большинстве случаев экранирования приходится иметь дело либо с переменными, либо с флуктуирующими и реже – действительно со статическими полями [71].

Теоретические и экспериментальные исследования ряда авторов показали, что форма экрана незначительно влияет на его эффективность. Главным фактором, определяющим качество экрана, являются радиофизические свойства материала и конструкционные особенности. Это позволяет при расчете эффективности экрана в реальных условиях пользоваться наиболее простым его представлением: сфера, цилиндр, плоскопараллельный лист и т.п. Такая замена реальной конструкции не приводит к сколько-нибудь значительным отклонениям реальной эффективности от расчетной, так как основной причиной ограничивающей достижение высоких значений эффективности экранирования является наличие в экране технологических отверстий (устройства ввода-вывода, вентиляции), а в экранированных помещениях – устройств жизнеобеспечения, связывающих помещение с внешней средой [71].

При экранировании реальных элементов, например трансформаторов, катушек индуктивности, проводов и т.д., обычно требуется одновременное экранирование от электрических и магнитных полей.

Наилучшую защиту как от электрического, так и от магнитного полей обеспечивают информационные линии связи типа экранированного бифиляра, трифиляра (трех скрученных вместе проводов из которых один используется в качестве электрического экрана), триаксиального кабеля (изолированного коаксиального кабеля, помещенного в электрический экран), экранированного плоского кабеля (плоского многопроводного кабеля, покрытого с одной или обеих сторон медной фольгой). Чтобы уменьшить уровень ПЭМИ, необходимо

особенно тщательно выполнять соединение оболочки провода (экрана) с корпусом аппаратуры. Вместе с тем соединение оболочки провода с корпусом в одной точке не ослабляет в окружающем пространстве магнитное поле, создаваемое протекающим по проводу током. Для экранирования магнитного поля необходимо создать поле такой же величины и обратного направления. С этой целью необходимо весь обратный ток экранируемой цепи направить через экранирующую оплетку провода. Для полного осуществления этого принципа необходимо, чтобы экранирующая оболочка была единственным путем для протекания отраженного тока [71].

Высокая эффективность экранирования обеспечивается при использовании витой пары, защищенной экранирующей оболочкой.

На низких частотах приходится использовать более сложные схемы экранирования – коаксиальные кабели с двойной оплеткой (триаксиальные кабели).

На более высоких частотах, когда толщина экрана значительно превышает глубину проникновения поля, необходимость в двойном экранировании отпадает. В этом случае внешняя поверхность играет роль электрического экрана, а по внутренней поверхности протекают обратные токи.

Длина экранированного провода должна быть меньше четверти длины самой короткой волны спектра сигнала, иначе его надо рассматривать как длинную линию, которую надо нагружать на волновое сопротивление. Для уменьшения взаимного влияния длину монтажных цепей следует выбирать наименьшей, для чего элементы высокочастотных схем, связанные между собой, следует располагать в непосредственной близости, а не экранированные провода высокочастотных цепей – при пересечении под прямым углом [71].

Экранированные провода и кабели следует применять в основном для соединения отдельных блоков и узлов друг с другом.

Кабельные экраны выполняются в форме цилиндра из сплошных оболочек, в виде спирально намотанной на кабель плоской ленты или в виде оплетки из тонкой проволоки. Экраны однослойные и многослойные.

Материал: свинец, сталь, медь, алюминий или их сочетание.

В области низких частот корпуса многоштырьковых низкочастотных разъемов являются экранами и должны быть надежно заземлены.

В области высоких частот коаксиальные кабели должны быть согласованы по волновому сопротивлению и иметь высокочастотные разъемы.

Наиболее экономичным способом экранирования информационных линий связи между устройствами ТСПИ считается групповое размещение их в экранирующем распределительном коробе.

Для полного экранирования проводов от электрических и магнитных полей необходимо добиваться, чтобы весь обратный ток протекал по экрану, т.е. чтобы токи, протекающие по экранируемому проводу и экрану, были равны между собой (рис. 1.43, *а*). Для этого необходимо выводы генератора и нагрузки подключать к проводу и экрану непосредственно без промежуточных проводников, а соединение с корпусом производить в одной точке, лучше со стороны приемника сигнала. При подключении общего провода генератора к

корпусу, а не к экрану (рис. 1.43, *б*) получается экранирование только от электрических полей. При отсутствии соединения экрана с общим проводом никакого экранирующего эффекта не возникает [61].

При соединении экрана с корпусом со стороны генератора или при соединении с корпусом через длинный провод эффективность экранирования падает за счет появления напряжения помех на этом проводе. Для экранирования проводов от низкочастотных наводок поверх экрана должна иметься изолирующая оболочка, исключающая случайные контакты с металлическими элементами корпуса изделия.

При замыкании экрана на корпус (рис. 1.43, *в*) нарушается магнитное экранирование части провода, расположенного между точкой замыкания экрана на корпус и нагрузкой. В этом случае довольно часто наблюдается, что при отключении соединения экрана около нагрузки уровень наводок снижается.

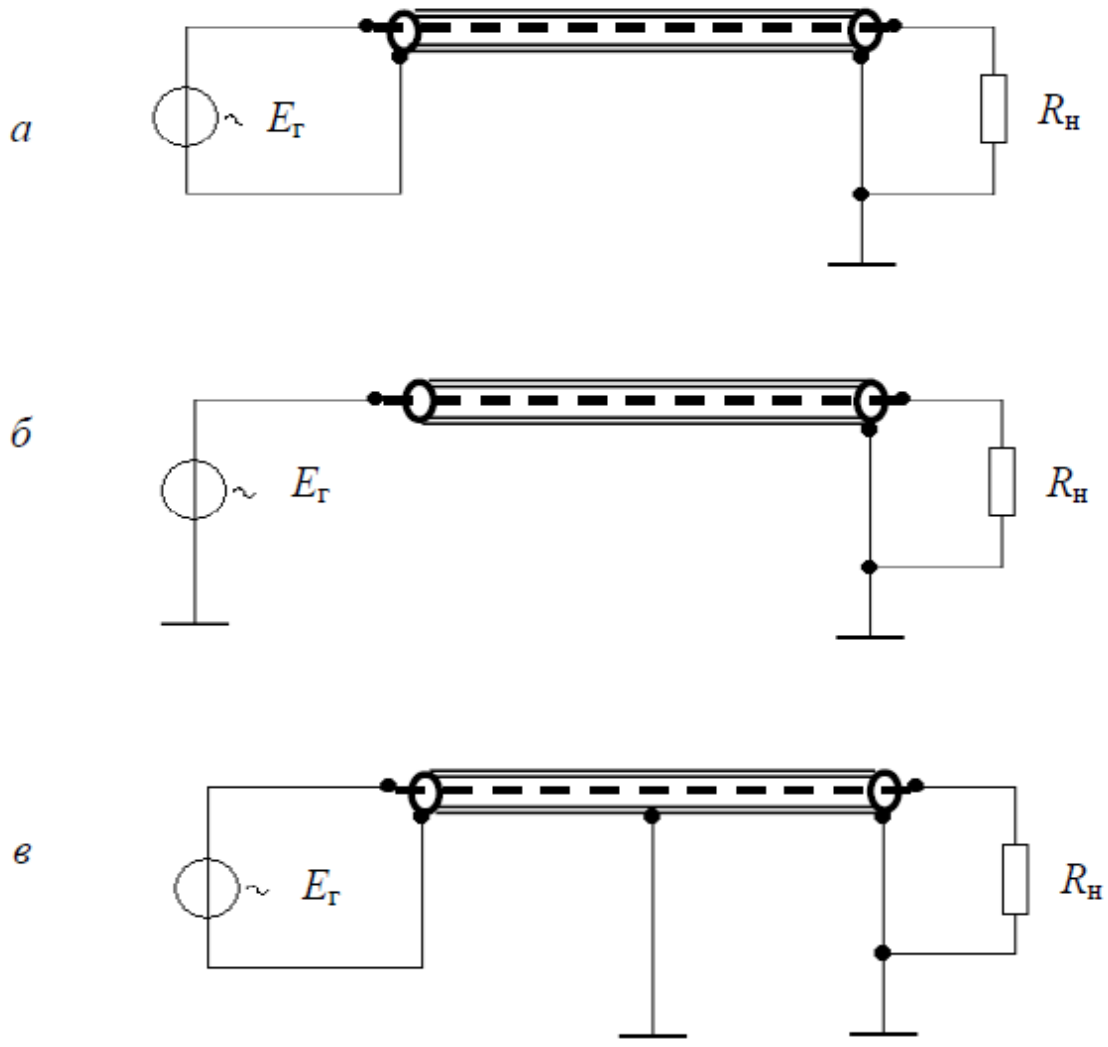


Рисунок 1.43 - Полное экранирование провода от электрических и магнитных полей (*а*), экранирование провода от электрических полей (*б*) и замыкание части экрана провода на корпус (*в*)

Если это явление наблюдается, необходимо найти и устранить замыкание экрана на корпус.

Экранироваться могут не только отдельные блоки аппаратуры и их соединительные линии, но и помещения в целом (рис. 1.44) [71].

В обычных (неэкранированных) помещениях основной экранирующий эффект обеспечивают железобетонные стены домов. Экранирующее свойство дверей и окон хуже. Для повышения экранирующих свойств стен применяются дополнительные средства, в том числе [71]:

- токопроводящие лакокрасочные покрытия или токопроводящие обои;
- шторы из металлизированной ткани;
- металлизированные стекла (например, из двуокиси олова), устанавливаемые в металлические или металлизированные рамы.

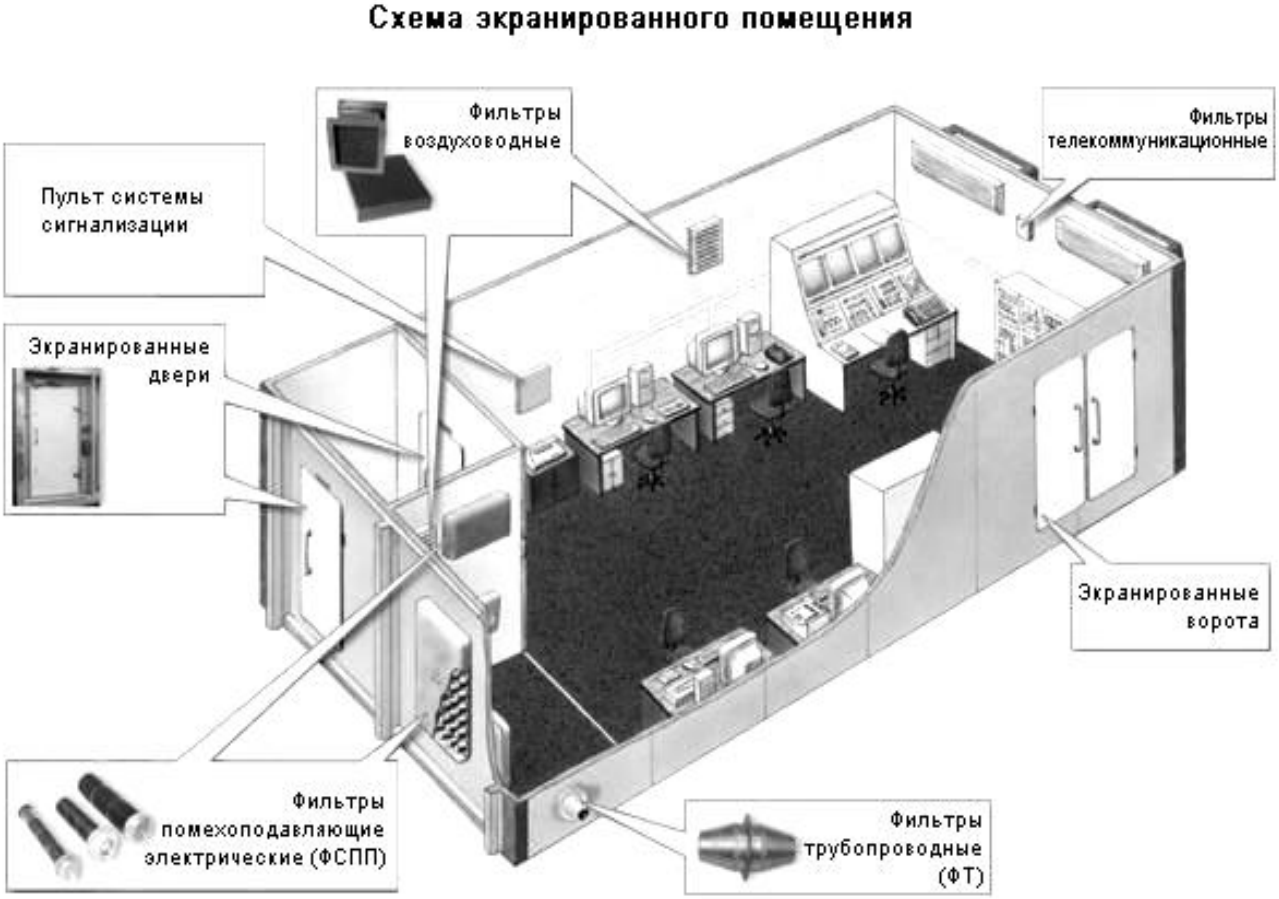


Рис. 1.44. Экранированное помещение

Экранировку электромагнитных волн более 100 дБ можно обеспечить только в специальных экранированных камерах (рис. 1.44), в которых электромагнитный экран выполнен в виде электрогерметичного стального корпуса, а для ввода электрических коммуникаций используются специальные фильтры.

Таким образом, экранированием электромагнитных волн возможно полностью обеспечить электромагнитную безопасность объекта. Однако

обеспечение требований по электромагнитной безопасности объекта, особенно в части, касающейся защиты информации от утечки по техническим каналам, созданным с применением специального оборудования (электроакустический канал, радиоканал, канал побочных электромагнитных излучений и наводок и т.д.), необходимо предусматривать на стадии разработки проекта объекта. Так, например, при проектировании в пределах объекта необходимо выделить зоны повышенной конфиденциальности – комнаты переговоров, технологические помещения, в которых циркулирует информация, предназначенная для служебного пользования, и т.п. В таких помещениях не должно быть окон, они должны иметь независимую систему электропитания, экранированные двери. При строительстве такого объекта возможно применение экранирующих материалов – шунгитобетона или бетона с электропроводящим наполнителем. Стены помещения отделываются гибкими экранами, например тканными коврами из аморфных материалов или электропроводящими тканями. В качестве экранирующей ткани возможно применение различных углетканей или металлизированных пленок. С внутренней стороны помещение облицовывается конструкционным радиопоглощающим материалом для предотвращения образования стоячих электромагнитных волн с частотами более 1 ГГц и для создания более комфортной экологической обстановки. В качестве радиопоглощающих материалов могут быть использованы специализированное пеностекло различных марок или сотовые конструкции. Коэффициент экранирования такого помещения может превышать 60 дБ в широком диапазоне частот [71].

Технологии позволяют производить качественное экранирование и уже существующих помещений, изначально не предназначавшихся для специального использования. Отделка стен многослойными гибкими экранами применима в большинстве случаев. При наличии окон они закрываются металлизированными пленками и шторами из экранирующих тканей.

В помещениях такого класса возможно применение гибких широкодиапазонных радиопоглощающих материалов. Для облицовки потолков помещения применяется наполненное пеностекло. Коэффициент экранирования достигает значения 20 дБ и больше [71].

1.5.3 Безопасность оптоволоконных кабельных систем

Важнейшими характеристиками волоконно-оптических систем передачи информации (ВОСПИ) являются [49]:

- слабое затухание сигнала и его меньшая зависимость от длины волны передаваемого информационного оптического сигнала, распределения мод и температуры кабеля;
- слабое искажение сигнала и его незначительная зависимость от спектральной ширины, распределения мод, амплитуды и длины волны

передаваемого информационного оптического сигнала, длины световода и температуры окружающей среды;

- малые потери на излучение и их незначительная зависимость от радиуса изгиба и температуры волоконного световода;
- более приемлемые физические параметры – вес, размер, общий объем;
- простота укладки, сращивания и ввода излучения в световод;
- высокая устойчивость к внешним воздействиям – влагостойкость, теплостойкость, стойкость к химической коррозии и к механическим нагрузкам.

Несмотря на перечисленные преимущества, ВОСПИ характеризуются также недостатками, главным из которых является возможность утечки информации за счет побочного электромагнитного излучения и наводок (ПЭМИН) как в радиочастотном, так и в оптическом диапазонах.

Оптоволокно – это обычное стекло, передающее электромагнитную энергию в инфракрасном диапазоне волн. Излучение наружу практически не просачивается. Эффективный перехват информации возможен только путем физического подключения к оптоволоконной линии. Однако если ВОСПИ рассматривать как систему, содержащую рабочие станции, серверы, интерфейсные карты, концентраторы и другие сетевые активные устройства, которые сами являются источником излучений, то проблема утечки информации становятся актуальной. Поэтому, принимая решения об использовании оптоволоконных кабельных систем (ОКС), необходимо учитывать эти факторы [71].

Волоконно-оптические кабели дифференцируются по размеру несущего волокна и оболочки – слоя стекла, отражающего свет [77].

Кроме. того, различают ОКС по режиму передачи: одномодовые и многомодовые кабели, а также по используемой длине волны (850–1550 нс) и применяемым источникам света (лазеры или светодиоды – LED).

Основным элементом оптоволоконного кабеля является внутренний сердечник из стекла или пластика (рис. 1.45, позиция 1). Диаметр и прозрачность стекловолокна определяют количество передаваемого им света.

Наиболее распространены следующие типы оптоволоконного кабеля:

- с сердечником 8,3 мк и оболочкой 125 мк;
- с сердечником 62,5 мк и оболочкой 125 мк;
- с сердечником 50 мк и оболочкой 125 мк;
- с сердечником 100 мк и оболочкой 145 мк.

Волоконно-оптические кабели толщиной в 8,3 микрона очень трудно соединить точно. Поэтому возможны монтажные ошибки, в том числе и трудно выявляемые при тестировании кабельной линии. Подобные дефекты можно устранить установкой дополнительных оптоволоконных повторителей (концентраторов), увеличивающих уровень электромагнитных излучений кабельной системы в целом. Однако в последнее время на рынке появились так называемые заказные кабельные комплекты, то есть кабели с уже смонтированными и проверенными в заводских условиях коннекторами, исключающими процедуры монтажа и тестирования линии в полевых условиях.

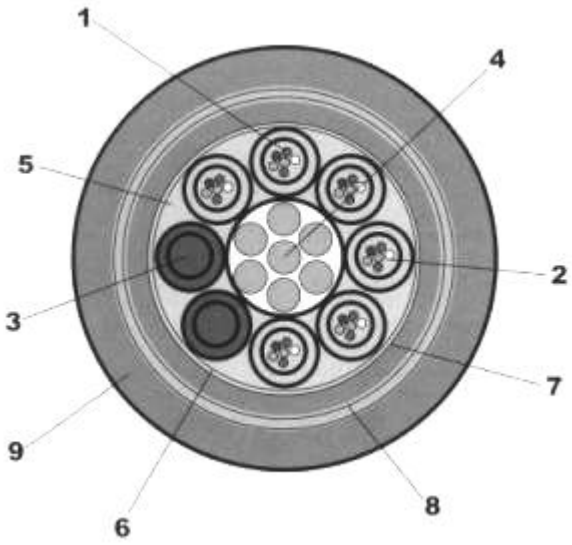


Рисунок 1.45 - Конфигурация оптоволоконного кабеля (на примере оптического городского кабеля производства фирмы Fujikara для прокладки в кабельной канализации, трубах, блоках, коллекторах, на мостах и в кабельных шахтах): 1 – оптическое волокно; 2 – внутримодульный гидрофобный заполнитель; 3 – кордель; 4 – центральный силовой элемент – стальной трос; 5 – гидрофобный заполнитель; 6 – скрепляющая лента; 7 –промежуточная оболочка из полиэтилена; 8 – броня из стальной гофрированной ленты; 9 – защитная оболочка из полиэтилена

Для оптоволоконного кабеля характерны следующие особенности:

- наличие центрального силового элемента;
- размещение в полимерной трубке-модуле;
- количество оптических волокон в одном модуле – от 1 до 12;
- заполнение пространства между модулями упрочняющими элементами – корделями из стеклонитей или нитей из кевлара и гидрофобным гелем;
- покрытие всех этих элементов и модулей промежуточной полимерной оболочкой;
- внешняя защита оболочки из полиэтилена или металла (возможно наличие двух защитных оболочек – металлической и полиэтиленовой).

Наряду с указанными общими особенностями оптоволоконные кабели различных фирм могут иметь дополнительные скрепляющие ленты, антикоррозийные и водозащитные обмотки, гофрированные металлические оболочки и т.д.

Как отмечалось выше, эффективным способом перехвата информации с оптоволоконных кабельных систем является непосредственное подключение к ним. Появилась информация о создании специальных дистанционно управляемых роботов, которые могут самостоятельно передвигаться по кабельным канализациям и подключаться к оптоволоконному кабелю для последующей передачи данных, циркулирующих в ОКС [71].

Для противодействия злоумышленникам, имеющим специальную технику, было предложено использовать внутренние силовые металлические конструкции

оптоволоконных кабелей в качестве сигнальных проводов. В этом случае невозможен доступ к оптоволокну без нарушения целостности силовых конструкций. Нарушение целостности приведет к срабатыванию сигнализации в центре контроля за ОКС. Дополнительного оборудования для реализации подобной охранной системы практически не требуется.

Параметры ОКС косвенно влияют на безопасность системы передачи данных в целом. Существуют одномодовый и многомодовый режимы передачи данных. По одномодовым волокнам передаются оптические сигналы с одной длиной волны. В многомодовых волокнах могут передаваться сигналы с различной длиной волны. Для совмещения нескольких оптических сигналов применяется так называемый волновой мультиплексор (Wave Division Multiplexer – WDM). WDM работает как призма. Сигналы с различной длиной волны комбинируются в нем, а затем пересылаются по одному из оптических волокон. Призма на приемном конце разлагает сигнал на волны исходной длины и направляет их на вход соответствующего оптического приемника. Применение мультиплексирования позволяет увеличить число возможных каналов передачи данных. Однако в многомодовых кабелях сигналы затухают сильнее, следовательно, расстояния между узлами регенерации должны быть значительно уменьшены, что делает систему более дорогой, более «излучающей» и менее защищенной [71].

В целом же затухание сигналов в оптоволоконном кабеле (до 5 дБ/км) немного меньше затухания электрического коаксиального кабеля. Это объясняется тем, что свет не излучается вне кабеля, как электрический сигнал в медных проводах. Очень важно и то, что с ростом частоты более 200 МГц оптоволоконные кабели имеют несомненное преимущество перед любыми электрическими кабелями. Поэтому для обеспечения безопасности информации целесообразна высокочастотная передача.

Затухание сигнала существенно увеличивается при разветвлении и ответвлении кабеля. В связи с этим предпочтительнее использовать однонаправленные кабели, что, в свою очередь, определяет предпочтительные топологии сети: «звезда» (с двумя разнонаправленными кабелями между центральным абонентом и каждым из периферийных) или кольцо (с одним однонаправленным кабелем).

Несмотря на малое затухание, волоконной оптике присуща другая проблема – хроматическая дисперсия. Волны света различной длины стекло пропускает по-разному, поэтому импульс света, проходя через кабель, «размывается». Получается эффект радуги – световой сигнал разделяется на цветовые компоненты. На расстоянии в несколько километров он может «залезть» в следующий бит, что приведет к потерям данных. Это нарушит их целостность, которая является наряду с конфиденциальностью и доступностью важнейшим аспектом информационной безопасности. В одномодовых кабелях передается свет одной частоты, поэтому здесь нет эффекта хроматической дисперсии.

Одно из возможных решений указанной проблемы – увеличение расстояния между соседними сигналами и соответственно сокращение скорости передачи, что не всегда допустимо. Однако исследования показали, что при генерации

сигнала в некоторой специальной форме дисперсионные эффекты почти исчезают, и сигнал можно передавать на тысячи километров. Сигналы в этой специальной форме называются силитонами [71].

К недостаткам оптоволоконного кабеля относятся меньшие механическая прочность и долговечность по сравнению с электрическим кабелем и снижение чувствительности при воздействии ионизирующих излучений.

Как было отмечено выше, компьютерные сети, построенные на базе оптоволоконных каналов, излучают в окружающее пространство конфиденциальные данные. Компания ITT Cannon NS&S провела ряд измерений уровня собственных излучений для оптоволоконной, экранированной и неэкранированной кабельных систем в специально оборудованных лабораториях. В результате оказалось, что на частотах до 70 МГц сеть на основе экранированной кабельной системы имеет самый низкий уровень собственных излучений. Это объясняется тем, что при хорошем заземлении экранирование не только снижает на несколько порядков собственные излучения кабелей, но и уменьшает электрический потенциал корпусов активных устройств. На частотах 70–100 МГц все системы показали скачкообразные кривые амплитудно-частотных характеристик уровня собственных излучений, хотя характер их у всех систем был примерно одинаковым. Появление пиков свидетельствует об образовании сложных колебательных контуров как в кабелях, так и в активном оборудовании [71].

Приведем пример влияния различных типов линий связи на вычислительную систему. При тестировании локальная вычислительная сеть функционировала в режиме передачи АТМ со скоростью 155 Мбит/с на линиях с незащищенной, с защищенной витой парой и с оптоволокном. В качестве воздействия рассматривалось радиочастотное поле с интенсивностью 3 В/м. Система на базе незащищенной витой пары характеризовалась высоким уровнем появления сбоев и в итоге вышла из строя. Локальная вычислительная сеть на оптоволокне имела сбои, но работала. И только локальная вычислительная сеть на основе защищенной витой пары была совершенно не подвержена помехам [71].

Таким образом, безопасность ОКС определяется самым «узким» местом телекоммуникационных систем – сетевым активным оборудованием.

Возможные каналы утечки информации в радиочастотном диапазоне известны и хорошо изучены. С начала 80-х годов велись работы по выявлению возможных каналов утечки информации в оптическом диапазоне частот. Для анализа возможных каналов утечки информации рассмотрим простейшую модель ВОСПИ (рис. 1.46) [49].

В качестве излучателя для ВОСПИ могут использоваться полупроводниковые устройства двух типов. Устройство простейшего типа – светоизлучающий диод имеет широкую диаграмму направленности излучения и поэтому пригоден для работы с многомодовыми волоконными световодами с большим диаметром сердцевины. Более сложные устройства – полупроводниковые лазеры излучают значительно лучше сколимированные пучки света и поэтому позволяют вводить сигнал более высокой мощности (в 10–100 раз) в многомодовые световоды, а также эффективно вводить сигнал в

одномодовые световоды с малым диаметром сердцевины. Светоизлучающие диоды вполне подходят для применения в информационных каналах и в системах связи с невысокой или умеренной пропускной способностью.

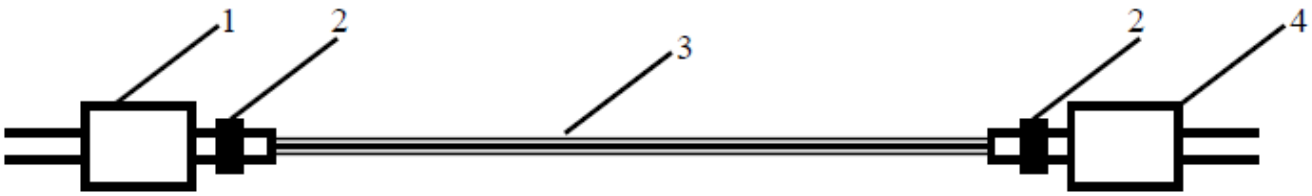


Рисунок 1.46 - Модель ВОСПИ: 1−излучатель; 2−оптический разъем; 3−оптическое волокно; 4−приемник

Утечка информации у излучателя возможна:

- за счет несоответствия геометрических размеров окна (микролинзы) светоизлучающего диода или полупроводникового лазера и торца (апертуры) волоконного световода;

- за счет «окон прозрачности» вокруг контактов на подложке, к которым подводится передаваемый информационный сигнал в радиочастотном диапазоне.

В качестве приемника в ВОСПИ, как правило, используются фотодиоды.

Утечка у приемника в оптическом диапазоне частот возможна:

- за счет несогласования геометрических размеров окна (микролинзы) фотодиода и торца волоконного световода;

- за счет «окон прозрачности» вокруг контактов на подложке, к которым подводится принимаемый информационный сигнал в радиочастотном диапазоне.

Для исключения утечки информации в оптическом диапазоне частот у излучателя и приемника необходимо, чтобы их конструкция с физической точки зрения представляла абсолютно «черное тело». Как правило, потери в оптических разъемах составляют 2,5–4,5 дБ.

Наибольший интерес представляет излучение информации с оптического волокна. Абсолютно все волоконные световоды обладают затуханием. Затухание света в волоконном световоде обусловлено поглощением и рассеянием в материале, рассеянием, связанным со световодной структурой и потерями на излучение. Рассеяние, связанное со световодной структурой, вызвано большей частью геометрическими неоднородностями поверхности раздела сердцевина-оболочка. Тщательно контролируя процесс изготовления, можно поддерживать уровень потерь на рассеяние этого типа ниже 1 дБ/км. Потери на излучение вызваны изгибами световода и при малых радиусах кривизны могут быть значительными [71].

Излучение из волоконного световода достигает особенно больших величин, если при изготовлении оптического кабеля используются световоды без мягкой амортизирующей пластиковой оболочки.

С точки зрения утечки информации наиболее опасными являются «оболочечные» и «вытекающие» моды, так как, имея доступ к данному типу оптического волокна, с помощью высокочувствительных фотоприемных

устройств (в качестве оптического объектива можно использовать микролинзы или специальное оптическое волокно, оптически согласованное с основным с помощью специально подобранной эмиссионной жидкости), можно принять передаваемый оптический сигнал [71].

При построении ВОСПИ для передачи конфиденциальной информации необходимо детально проанализировать условия эксплуатации, гриф информации, выбрать тип оптического кабеля, позволяющий осуществить защиту информации от возможной утечки за счет побочного излучения в оптическом диапазоне частот. Помимо конструктивных средств защиты информации можно использовать и активную защиту, в частности зашумление в оптическом диапазоне и квантовую криптографию [71].

1.5.4 Заземление технических средств и подавление информационных сигналов в цепях заземления

Необходимо помнить, что экранирование ТСПИ и соединительных линий эффективно только при правильном их заземлении. Поэтому одним из важнейших условий по защите ТСПИ является правильное заземление этих устройств.

В настоящее время существуют различные типы заземлений. Наиболее часто используются одноточечные, многоточечные и комбинированные (гибридные) схем [74].

На рис. 1.47 показана наиболее простая последовательная одноточечная схема заземления, применяемая на низких частотах. Однако ей присущ недостаток, связанный с протеканием обратных токов различных цепей по общему участку заземляющей цепи. Вследствие этого возможно появление опасного сигнала в посторонних цепях [71].

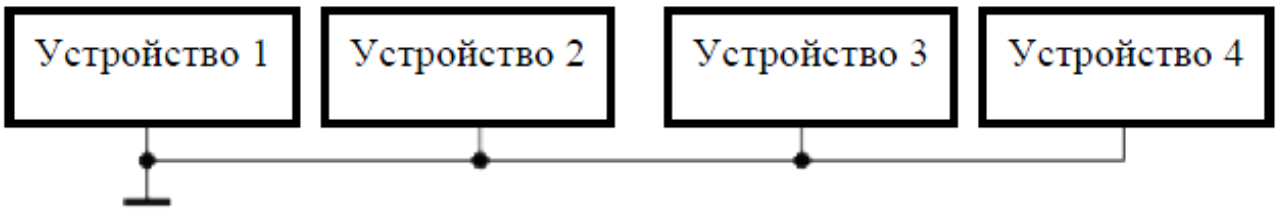


Рисунок 1.47 - Одноточечная последовательная схема

В одноточечной параллельной схеме (рис. 1.48) этого недостатка нет. Однако такая схема требует большого числа протяженных заземляющих проводников, из-за чего может возникнуть проблема с обеспечением малого сопротивления участков заземления. Применяется на низких частотах.

Многоточечная схема заземления (рис. 1.49) свободна от выше указанных недостатков, но требует принятия мер для исключения замкнутых контуров. Применяется на высоких частотах.

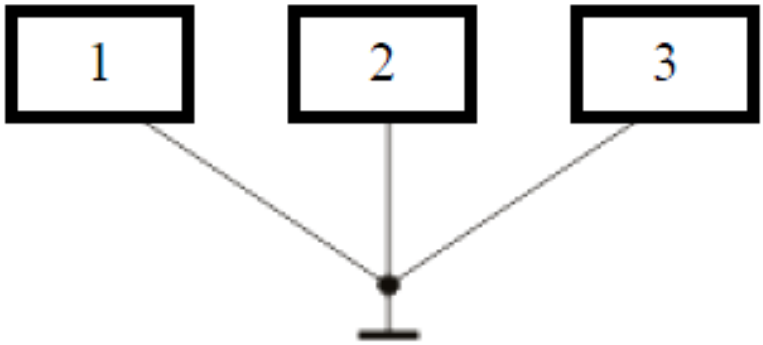


Рисунок 1.48 - Одноточечная параллельная схема

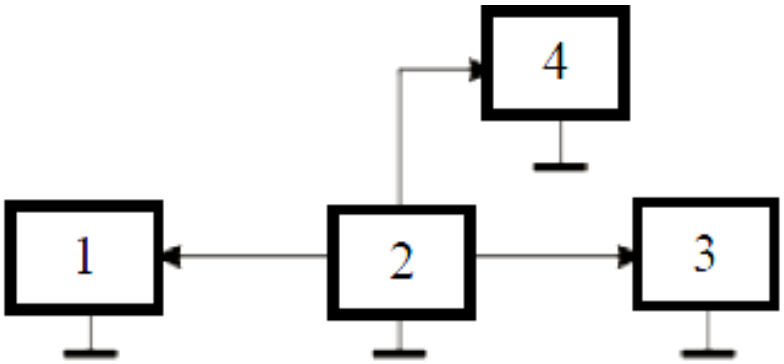


Рисунок 1.49 - Многоточечная схема

Комбинированные схемы представляют собой сочетание названных [71]:

- система заземления должна включать общий заземлитель, заземляющий кабель, шины и провода, соединяющие заземлитель с объектом;
- сопротивление заземляющих проводников, а также земляных шин должны быть минимальными;
- каждый заземленный элемент должен быть присоединен к заземлителю при помощи отдельного ответвления;
- в системе заземления должны отсутствовать замкнутые контуры;
- следует избегать использования общих проводников в системе экранируемых заземлений, защитных заземений и сигнальных цепей;
- минимальное сопротивление контактов (лучше пайка);
- контактные соединения должны исключать возможность образования оксидных пленок, вызывающих нелинейные явления;
- контактные соединения должны исключать возможность образования гальванических пар, вызывающих коррозию;
- запрещается использовать в качестве заземлителей нулевые фазы, металлические оболочки подземных кабелей, металлические трубы водо- и теплоснабжения.

Сопротивления заземления определяются качеством грунта. Орошение почвы вокруг заземления 5%-м соляным раствором снижает сопротивление в 5–10 раз.

Для эффективного подавления информативных сигналов в цепях заземления и электропитания применяют электрическое зашумление от генераторов шума.

1.5.5 Фильтрация информационных сигналов

Одним из методов локализации опасных сигналов, циркулирующих в технических средствах и системах обработки информации, является фильтрация. В источниках электромагнитных полей и наводок фильтрация осуществляется с целью предотвращения распространения нежелательных электромагнитных колебаний за пределами устройства – источника опасного сигнала [71].

Для фильтрации сигналов в цепях питания ТСПИ используются разделительные трансформаторы и помехоподавляющие фильтры [45, 74].

Разделительные трансформаторы должны обеспечивать разводку первичной и вторичной цепей по сигналам наводки. Проникновение наводок во вторичную обмотку объясняется наличием нежелательных резистивных и емкостных цепей связи между обмотками.

Для уменьшения этих связей часто применяется внутренний экран, выполняемый в виде заземленной прокладки или фольги, укладываемой между первичной и вторичной обмотками. С помощью этого экрана наводка первичной обмотки замыкается на землю. Однако электромагнитное поле вокруг экрана также может служить причиной наводки.

Разделительные трансформаторы решают задачи:

- разделение по цепям питания источников и рецепторов наводки, если они подключаются к одним и тем же цепям переменного тока;
- устранение ассиметричных наводок;
- ослабление симметричных наводок на вторичную обмотку.

Разделительный трансформатор со специальными средствами экранирования и развязки обеспечивают ослабление информационного сигнала наводки на 126 дБ.

Помехоподавляющие фильтры обеспечивают ослабление нелинейных сигналов в разных участках частотного диапазона. Основное значение фильтров – пропускать без значительного ослабления сигналы с частотами, лежащими в рабочей полосе, и подавлять сигналы за пределами полосы.

Количественная величина ослабления фильтра определяется логарифмом амплитудно-частотных характеристик [71]

$$A = 20lg\left(\frac{U_1}{U_2}\right), \qquad (1.3)$$

где U_1 – напряжение опасного сигнала на входе фильтра, U_2 – напряжение опасного сигнала на выходе фильтра.

Важнейшим условием защиты информации в технических средствах является создание специализированной базы технологических компонентов – помехоподавляющих изделий, необходимых для принятия схемотехнических мер по минимизации паразитных генераций и побочных излучений на этапе разработки любого электронного устройства.

Побочные излучения обусловлены тем, что в генераторных, усилительных и других функциональных каскадах электронных устройств могут возникать паразитные генерации и наводки. Если при разработке аппаратуры не принять мер подавления указанных процессов непосредственно в местах их возникновения, создаются условия для устойчивого генерирования, усиления и возникновения побочных излучений, уровень которых может превышать нормы допустимых радиопомех.

Излучения от устройств электронно-вычислительной техники модулированы полезным сигналом, существуют в виде полезных гармоник в широком диапазоне частот, распространяются как кондуктивно, так и в виде излучаемых электромагнитных помех и несут в себе сигнал с тем же информационным содержанием, что и обрабатываемые сигналы. Такие излучения могут быть приняты и выведены на экран монитора аппаратуры перехвата. Устройства средств вычислительной техники могут быть как источником, так и рецептором – устройством, восприимчивым к внешним электромагнитным помехам, и могут служить переизлучателем этих помех.

Побочные излучения и кондуктивные помехи создают каналы утечки информации, обрабатываемой в технических средствах.

Технические меры борьбы с электромагнитными помехами включают в себя меры подавления паразитных генераций – источников побочных излучений, экранирование аппаратуры от внешних электромагнитных полей и фильтрацию кондуктивных помех.

Фильтрация является основным и эффективным средством подавления (ослабления) кондуктивных помех в цепях электропитания, в сигнальных цепях интерфейса и на печатных платах, в проводах заземления. Помехоподавляющие фильтры позволяют снизить кондуктивные помехи, как от внешних, так и от внутренних источников помех.

Применение помехоподавляющих элементов позволяет оптимизировать схемотехнические и конструкторско-технологические решения с целью минимизации или полного устранения паразитных генераций и побочных излучений, снизить восприимчивость аппаратуры к внешним электромагнитным полям и импульсным сигналам, устранить возможные каналы утечки информации.

В соответствии с расположением полосы пропускания фильтра относительно полосы помехоподавления в частотном спектре различают четыре класса помехоподавляющих фильтров, амплитудно-частотные характеристики которых показаны на рис. 1.50 [45, 52]:

- фильтры нижних частот (низкочастотные) – ФНЧ, пропускающие сигналы в диапазоне частот от ω1 =0 до ω2 (рис. 1.50, *1*);

- фильтры верхних частот (высокочастотные) – ФВЧ, пропускающие сигналы в диапазоне частот от ω1 до ω2 =∞ (рис. 1.50, *2*);

- полосовые (полосно-пропускающие) – ПФ, пропускающие сигналы в диапазоне частот от ω1 до ω2 (рис. 1.50, *3*);

- заграждающие или режекторные (полосно-задерживающие) ЗФ, пропускающие сигналы в диапазоне частот от 0 до ω1 и от ω2 до ∞ (рис.1.50, *4*)

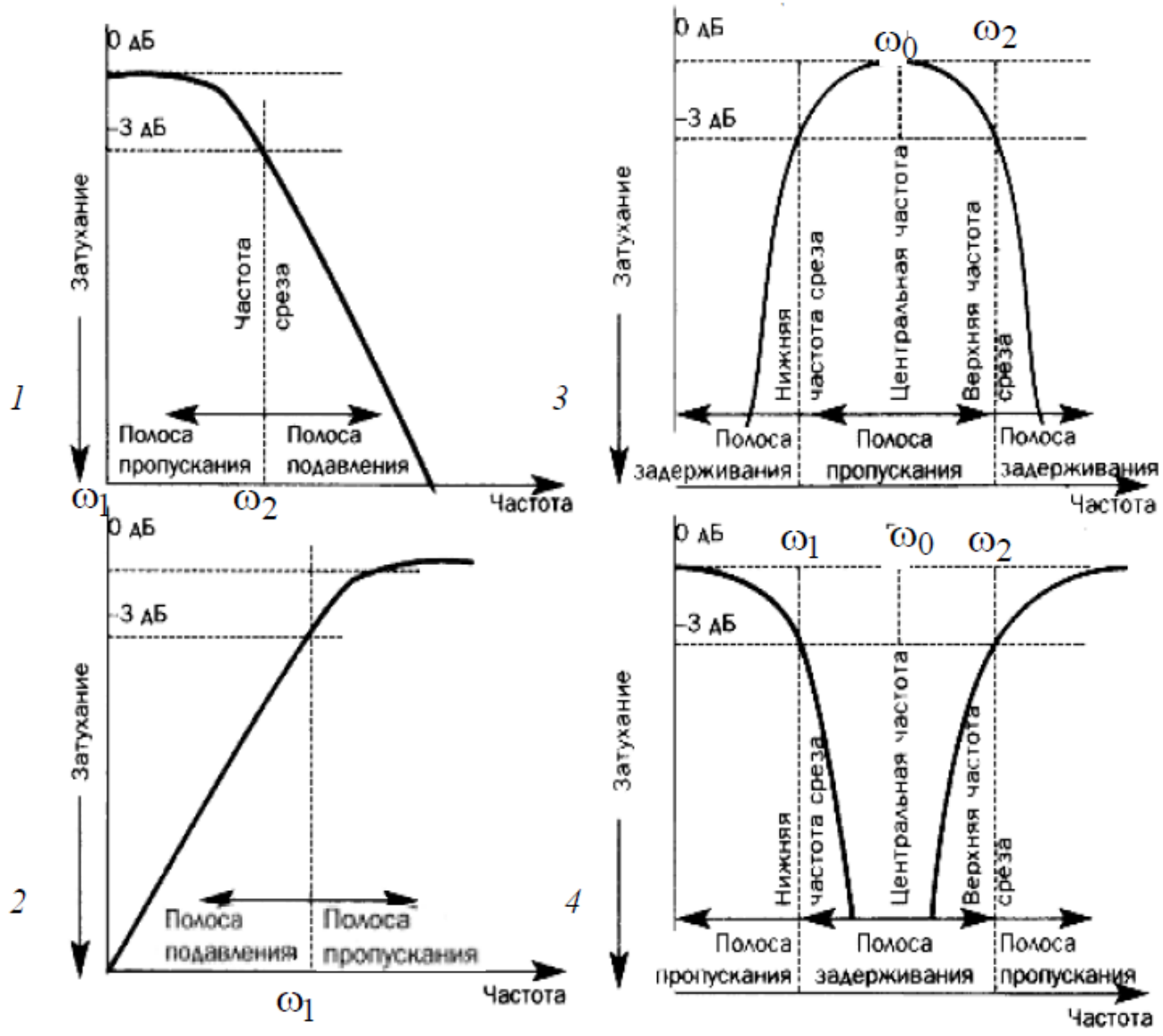


Рисунок 1.50 - Амплитудно-частотные характеристики помехоподавляющих фильтров: *1* – фильтра нижних частот, *2* – фильтра верхних частот, *3* – полосового фильтра, *4* – режекторного фильтра

В зависимости от типов элементов, из которых составлены фильтры, их делят на:

- реактивные, состоящие из элементов *L* и *C*;

- пьезоэлектрические, состоящие из кварцевых пластин;

- безындукционные пассивные, состоящие из элементов *r* и *C*.

Выбор необходимого типа фильтра зависит от электрической характеристики системы, в которую он должен быть установлен, требований по эффективности подавления помех, в том числе частоты среза и верхней предельной частоты ослабления, т.е. частотных характеристик фильтруемой цепи, а также требований, определенных условиями эксплуатации и от реальных ограничений по установке фильтра в аппаратуре. Все эти факторы увязываются с электрическими характеристиками фильтра [71].

1.5.6 Пространственное и линейное зашумление

Фильтрация относится к пассивным методам защиты. Когда фильтрация недостаточна по эффективности на границе контролируемой зоны, то прибегают к активным методам защиты, основанным на создании помех техническими средствами, что снижает отношение сигнал/шум.

Система пространственного зашумления должна обеспечивать [76]:

- электромагнитные помехи в диапазоне частот возможных побочных излучений ТСПИ;
- нерегулярную структуру помех;
- уровень создаваемых помех на электрический ток и по магнитной составляющей должен обеспечивать минимальное значение сигнал/шум;
- за счет выбора типа антенны помехи должны иметь горизонтальную и вертикальную поляризацию.

В системах пространственного зашумления в основном используются помехи типа «белого шума» или «синфазные помехи».

«Синфазные помехи» с основном применяются для защиты ЭВМ. В них в качестве помехового сигнала используются импульсы случайной амплитуды, совпадающие по форме и времени существования с импульсами полезного сигнала. Вследствии этого по своему спектральному составу помеховый сигнал аналогичен спектру побочных электромагнитных излучений ПЭВМ. То есть, сигнал зашумления генерирует «имитационную помеху», по спектральному составу соответствующему спектральному сигналу [71].

Широкополосный сигнал помехи «белый шум» имеет равномерно распределенный энергетический спектр во всем рабочем диапазоне, существенно превышающий уровни побочных излучений. Такие системы применяются для защиты ЭВМ, систем звукоусиления и звукового сопровождения, систем внутреннего телевидения.

Системы линейного зашумления применяются для маскировки наведенных опасных сигналов в посторонних проводниках и соединительных линиях ВТСС, выходящих за пределы контролируемой зоны.

В простейшем случае система линейного зашумления представляет собой генератор шумового сигнала, формирующий шумовое маскирующее напряжение с заданными спектральными, временными и энергетическими характеристиками,

который гальванически подключается в зашумляемую линию (посторонний проводник). На практике наиболее часто подобные системы используются для зашумления линий электропитания (осветительной и розеточной сети).

Ниже приведены внешний вид и описание некоторых сетевых генераторов шума [71].

Генератор шума сетевой СОПЕРНИК (рис. 1.51) предназначен для обнаружения и подавления (в автоматическом режиме) устройств несанкционированного съема информации, использующих для передачи данных сеть 220 В.

Прибор предназначен для постоянной работы в дежурном режиме. СОПЕРНИК постоянно сканирует и анализирует сеть. При появлении в сети высокочастотной составляющей загорается красная светодиодная линейка, показывающая уровень сигнала, присутствующего в сети, и сразу же загорается зеленая светодиодная линейка, показывающая уровень шумового сигнала, генерируемого прибором в качестве противодействия. Автоматически включается вентилятор прибора, обеспечивающая нормальный режим работы. При понижении в сети высокочастотного сигнала ниже определенного уровня прибор автоматически переходит в ждущий режим.

Прибор обеспечивает высокую эффективность защиты и не требует специальной технической подготовки пользователя.

Генератор шума SI-8001 (рис. 1.51) предназначен для защиты электросети переменного тока 220В / 50Гц от несанкционированного использования при передаче информации с помощью специальных технических средств. Принцип действия прибора основан на создании маскирующего сигнала (шума) в электросети в диапазоне частот от 5 кГц до 10 МГц. Генератор не оказывает влияния на работу персональных компьютеров и бытовой техники.

Рисунок 1.51 - Генераторы шума сетевые СОПЕРНИК и SI-8001

Генератор шума по сети электропитания IMPULSE (рис. 1.52) предназначен для блокирования каналов негласного съема информации из помещений по сети

220 В/50 Гц и линиям заземления. Позволяет нейтрализовать аппаратуру, использующую сеть электропитания в качестве канала передачи информации.

Рисунок 1.52 - Генераторы шума сетевые IMPULSE и NG-401

Свипирующий генератор белого шума сетевой NG-401 (рис. 1.52) предназначен для защиты электросетей переменного тока 220 В, 50 Гц от несанкционированного их использования для передачи речевой информации. Принцип действия основан на подаче в защищаемую сеть сложного шумоподобного сигнала с цифровым формированием. Модификация изделия «NG-402» позволяет защищать одновременно три фазы силовой линии [71].

1.5.7 Способы предотвращения утечки информации через ПЭМИН ПК

В качестве технических способов исключения возможностей перехвата информации за счет ПЭМИН ПК можно перечислить следующие [71]:

- доработка устройств ВТ с целью минимизации уровня излучений;
- электромагнитная экранировка помещений, в которых расположена вычислительная техника;
- активная радиотехническая маскировка (зашумление).

Доработка устройств ВТ осуществляется используя различные радиопоглощающие материалы и схемотехнические решения. При этом удается существенно снизить уровень излучений ВТ. Стоимость подобной доработки зависит от размера требуемой зоны безопасности и колеблется в пределах 20–70% от стоимости ПК. Электромагнитная экранировка помещений в широком диапазоне частот является сложной технической задачей, требует значительных капитальных затрат и не всегда возможна по эстетическим и эргономическим соображениям. Активная радиотехническая маскировка предполагает формирование и излучение в непосредственной близости от ВТ маскирующего сигнала [71].

Различают энергетический и неэнергетический методы активной маскировки. При энергетической маскировке с помощью генераторов шума излучается широкополосный шумовой сигнал с уровнем, существенно

превышающим во всем частотном диапазоне уровень излучений ПК. Одновременно происходит наводка шумовых колебаний в отходящие цепи.

Из устройств активной энергетической маскировки наиболее известны [71]: «Гном», «Шатер», «ИнейТ», «Гамма». Их стоимость достигает 25–30% от стоимости ПК. При установке такого устройства необходимо убедиться в достаточности мер защиты, так как в его частотной характеристике возможны провалы. Для этого потребуется привлечение специалистов с соответствующей измерительной аппаратурой.

Статистические характеристики сформированных генератором маскирующих колебаний близки к характеристикам нормального белого шума.

Более дешевыми являются генераторы шума ГШ-1000 и ГШ-К-1000. Генератор шума ГШ-1000 выполнен в виде отдельного блока с питанием от сети 220 В (рис. 4.19) и предназначен для общей маскировки ПЭМИ персональных компьютеров, компьютерных сетей и комплексов на объектах АСУ и электронно-вычислительной техники первой, второй и третьей категорий.

Ш-К-1000 изготавливается в виде отдельной платы (рис. 1.53), встраиваемой в свободный слот системного блока персонального компьютера, и питается напряжением 12В от общей шины компьютера.

Диапазон рабочих частот генераторов шума 0,01–1000 МГц. Спектральные характеристики обеих рассматриваемых моделей идентичны.

Возможности энергетической активной маскировки могут быть реализованы только в случае, если уровень излучений ПК существенно меньше норм на допускаемые радиопомехи от средств ВТ. В противном случае устройство активной энергетической маскировки будет создавать помехи различным радиоустройствам, расположенным поблизости от защищаемого средства ВТ, и потребуется согласование его установки со службой радиоконтроля [71].

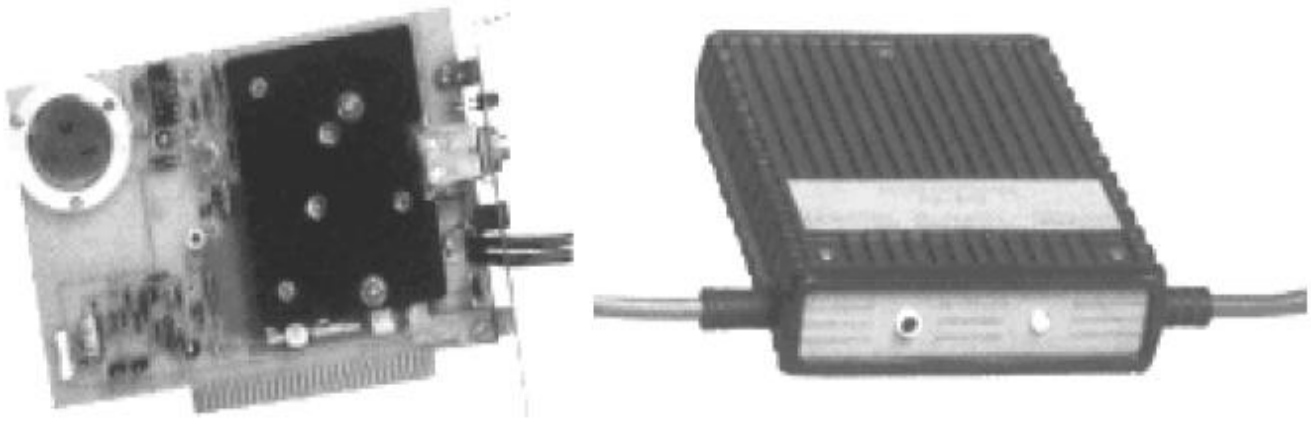


Рисунок 1.53 - Генераторы шума ГШ-К-1000 и ГШ-1000

Неэнергетический (статистический) метод активной маскировки заключается в изменении вероятностной структуры сигнала, принимаемого приемником злоумышленников, путем излучения специального маскирующего сигнала. Исходной предпосылкой в данном методе является случайный характер

электромагнитных излучений ПК. Для описания этих излучений используется теория марковских случайных процессов. В качестве вероятностных характеристик применяются матрицы вероятностей переходов и вектор абсолютных вероятностей состояний. Сформированный с помощью оригинального алгоритма сигнал излучается в пространство компактным устройством, которое может устанавливаться как на корпусе самого ПК, так и в непосредственной близости от него. Уровень излучаемого этим устройством маскирующего сигнала не превосходит уровня информативных электромагнитных излучений ПК, поэтому согласования установки маскирующего устройства со службой радиоконтроля не требуется. Более того, подобные устройства в отличие от устройств активной энергетической маскировки не создают ощутимых помех для других электронных приборов, находящихся рядом с ними, что также является их неоспоримым преимуществом [71].

Установка и включение устройств активной маскировки, реализующих статистический метод, могут быть произведены без каких-либо трудоемких монтажных работ. Устройство не требует квалифицированного обслуживания, его надежная работа гарантируется встроенной схемой контроля работоспособности.

Следует отметить, что в случаях: доработки устройств ВТ, электромагнитной экранировки помещений и активной энергетической маскировки – показателем защищенности является отношение сигнал/шум, обеспечиваемое на границе минимально допустимой зоны безопасности. Максимально допустимое отношение сигнал/шум рассчитывается в каждом конкретном случае по специальным методикам. При активной радиотехнической маскировке с использованием статистического метода в качестве показателя, характеризующего защищенность, применяется матрица вероятностей переходов. В случае идеальной защищенности эта матрица будет соответствовать матрице вероятностей переходов шумового сигнала, все элементы которой равны между собой [71].

Несмотря на то, что для большинства руководителей предпринимательских структур утечка информации с ограниченным доступом из используемой ВТ через ПЭМИН кажется маловероятной, такой канал перехвата информации все же существует, а это значит, что рано или поздно кто-то им все-таки воспользуется. Особую остроту эта проблема приобретает для коммерческих фирм, офисы которых занимают одну или несколько комнат в здании, где кроме них размещаются другие организации. Универсального, на все случаи жизни, способа защиты информации от перехвата через ПЭМИН ПК, конечно же, не существует. В каждом конкретном случае специалистами должно приниматься решение о применении того или иного способа защиты, а возможно и их комбинации. И все же для большинства малых и средних фирм оптимальным способом защиты информации с точки зрения цены, эффективности защиты и простоты реализации представляется активная радиотехническая маскировка [71].

1.5.8 Устройства контроля и защиты слаботочных линий и сети

При решении задачи обеспечения безопасности помещения необходимо учитывать, что злоумышленник может использовать телефонные и электросиловые линии, проходящие в здании, следующим образом [71].

Электросиловые линии используются для подслушивания разговоров в помещениях, через которые проходит линия. Как правило, линия используется в качестве источника питания подслушивающих устройств, передающих информацию из помещения по радиоканалу. Линия может использоваться и в качестве проводного канала. Достоинство такого канала передачи является большая, чем у радиоканала, скрытность, недостатком – что приемник информации необходимо подключать к той же линии, причем не дальше первой трансформаторной подстанции.

При использовании электросиловой линии в качестве источника питания подслушивающее устройство может быть подключено параллельно или последовательно линии. Параллельное подключение более предпочтительно, так как при нем подслушивающие устройство для питания использует напряжение линии и может работать практически в любое время (напряжение к линии приложено практически постоянно).

Для увеличения скрытности устройства при таком подключении могут применяться так называемые «сторожевые устройства», отключающиеся от сетевых проводов на несколько часов при кратковременном пропадании сетевого напряжения в линии. Последовательное подключение менее удобно для работы подслушивающего устройства, так как в этом случае для питания используется ток линии, а он появляется в линии только при подключении нагрузки.

Телефонные линии используются [71]*:*

- для подслушивания телефонных разговоров (линия используется, как источник информационного сигнала, и может при этом использоваться как источник питания);
- для подслушивания разговоров в помещениях, вблизи которых проходит телефонная линия (телефонная линия используется как скрытный канал передачи информации в любое место, где есть телефон, и как источник питания);
- в качестве бесплатного канала телефонной связи (междугородные переговоры за чужой счет) и для проникновения в банковскую компьютерную сеть для присвоения денег (в том случае, если используется телефонная линия для пересылки финансовых документов).

При подслушивании телефонных разговоров специальное радиоэлектронное устройство может быть подключено в любом доступном для злоумышленников месте (в телефонном аппарате; в помещениях, в которых проходит линия, в распределительных коробках и шкафах здания; в узловых распределительных шкафах городской телефонной сети; на АТС) и подключаться параллельно линии (гальванически) или последовательно (гальванически или индуктивно) [71].

При подслушивании разговоров в помещении специальное радиоэлектронное устройство может быть подключено только в помещении,

которое хотят прослушать, и включаться только параллельно линии (гальванически), а работать может только в то время, когда телефоном не пользуются.

В качестве канала телефонной связи, а также для проникновения в банковскую систему, специальное радиоэлектронное устройство может быть подключено в любом доступном для злоумышленников месте, устройство может включаться только параллельно линии (гальванически) и работать только в то время, когда телефонной линией не пользуются.

В зависимости от типа анализатора, используемого для контроля на закладные устройства силовых и телефонных линий, рекомендуются типовые схемы обследования линий [71].

При применении анализатора линий КОМ-2М рекомендуются типовые схемы его подключения, показанные на рис. 1.54, 1.55, 1.56 и 1.57.

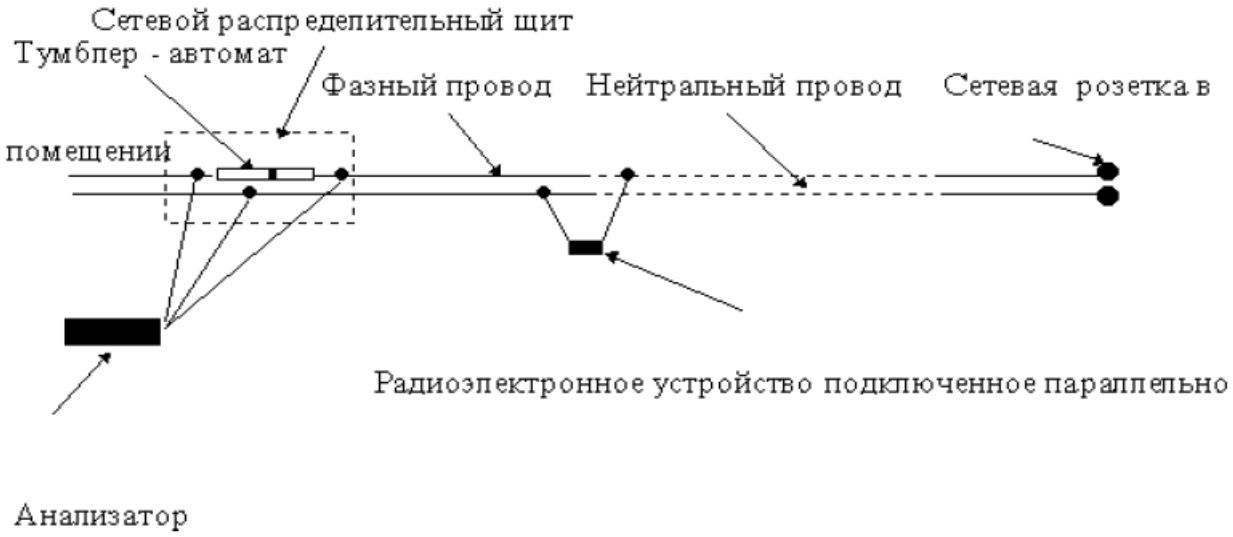


Рисунок 1.54 - Схема обследования электросиловой линии в режиме холостого хода

Анализатор линий КОМ-2М предназначен для обследования электросиловых и слаботочных линий (в том числе телефонных), с целью обнаружения микропотребляющих блоков питания, передатчиков и приемников подслушивающих устройств, негласно установленных на линиях [71].

Принцип действия анализатора основан на измерении и анализе следующих параметров линий:

- вольтамперной характеристики линии в режимах «холостого хода» (хх) и «короткого замыкания» (кз);
- импеданса линии в режиме «холостого хода»;
- тока утечки электросиловой линии на частоте 50 Гц;
- сопротивления изоляции линии на постоянном токе.

Вольтамперные характеристики линии анализируются так называемыми методами «нелинейной локации» с приемом второй и третьей гармонических составляющих испытательного напряжения.

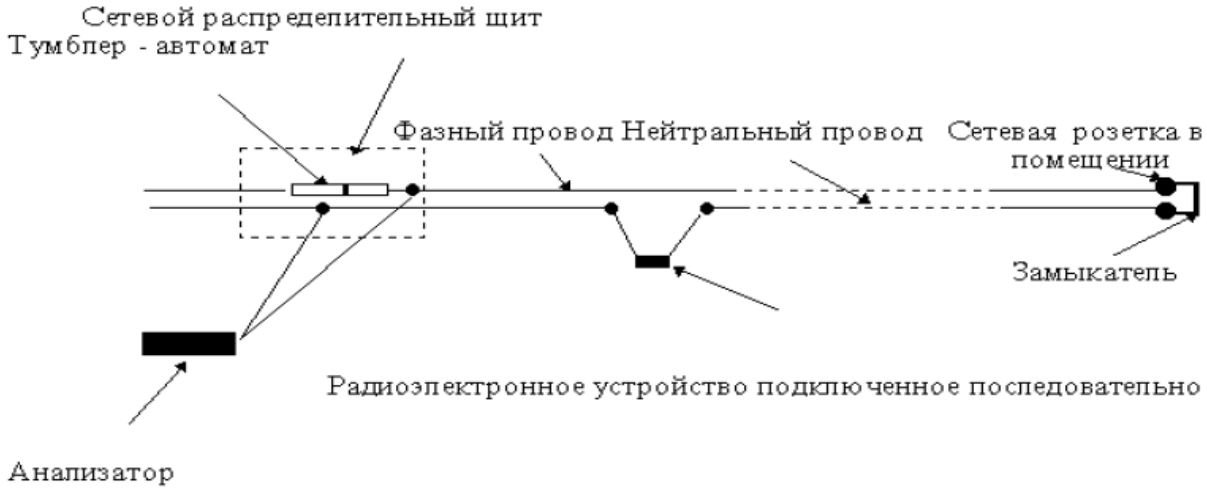


Рисунок 1.55 - Схема обследования электросиловой линии в режиме короткого замыкания

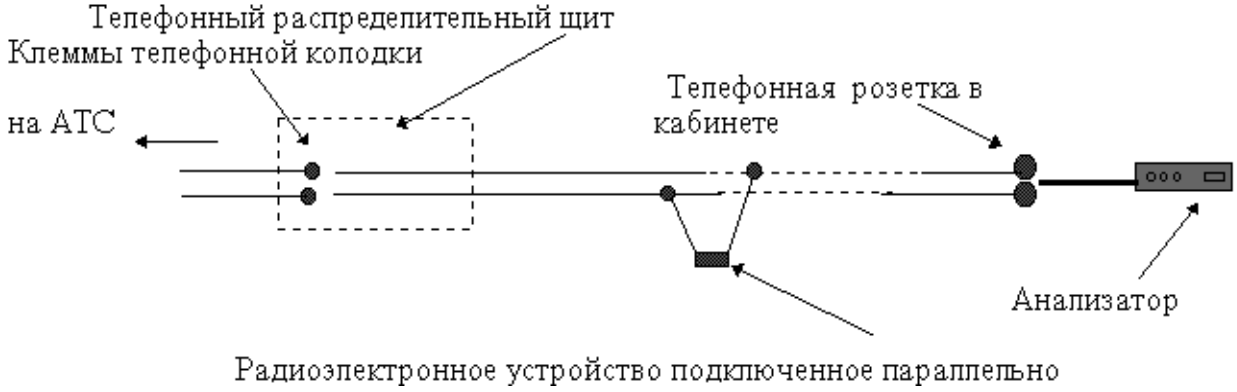


Рисунок 1.56 - Схема обследования телефонной линии в режиме холостого хода

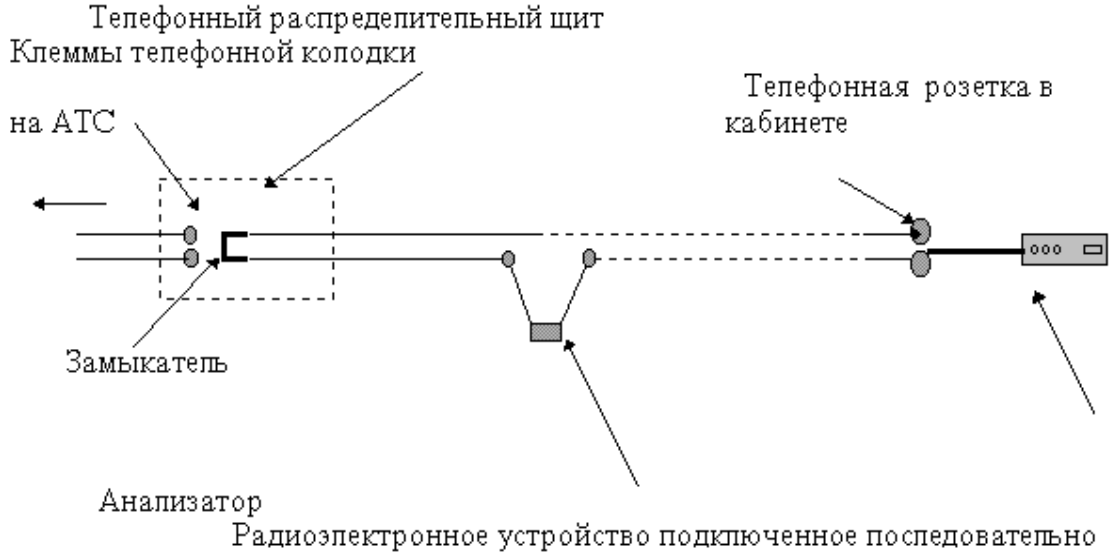


Рис. 1.57 - Схема обследования телефонной линии в режиме короткого замыкания

Импеданс линии (точнее его отклонение от типовых значений) анализируется методом измерения переходных процессов импульсных сигналов в линиях.

Ток утечки и сопротивления изоляции измеряются стандартными методами, применяемыми в современных мультиметрах.

Определение прохождения обследуемой телефонной пары в телефонном распределительном шкафу производится путем подачи в линию специального тестового сигнала и фиксация его индуктивным датчиком приемника тестового сигнала в распределительном шкафу.

Анализатор характеризуется следующими техническими возможностями:

- позволяет обнаруживать блоки питания специальных радиоэлектронных устройств, подключенных параллельно к линии, с мощностью потребления – 10 мкВт и более, оборудованных сторожевыми устройствами;
- позволяет обнаруживать блоки питания специальных радиоэлектронных устройств, подключенных последовательно к электросиловой линии, с мощностью потребления – 100 мкВт и более;
- напряжение испытательного сигнала (220 ± 20)В на частоте 50 Гц;
- чувствительность на второй и третьей гармонике испытательного напряжения не хуже – 10 мкВ;
- анализатор позволяет фиксировать отклонения импеданса линии от типового значения, при подключении к линии последовательно соединенных конденсатора с емкостью 100 пФ и более и резистора с сопротивлением 1 МОм;
- диапазон измерения токов утечки от 0.1 до 200 мА;
- диапазон измерения сопротивления изоляции от 100 кОм до 20 Мом;
- анализатор позволяет определять нахождение обследуемой телефонной пары в телефонных распределительных шкафах;
- длина обследуемых линий – до 100 метров;
- питание от сети переменного тока напряжением 220 В частотой 50 Гц.

Для защиты информации от утечки по проводным линиям разработаны многочисленные устройства, часть из которых рассматривается ниже.

Коммутатор-конвертер для поиска и анализ сигналов в сети 220 В и проводных линиях RS/KL (рис. 1.58) расширяет возможности комплексов обнаружения и локализации радиомикрофонов RS turbo M, построенных на базе сканирующих радиоприемников. Он дает возможность сканеру принимать низкочастотные сигналы, которые передаются по проводам сети переменного тока с напряжением 220 В и по проводным, в частности, по телефонным линиям без модуляции или на несущих частотах от 600 Гц до 10 МГц. Входы коммутатора-конвертера 1,2,3 предназначены для анализа трёх фаз электропитания, входы 4, 5, 6, 7 – для анализа слаботочных линий [71].

Необходимый режим работы выбирается в настройках программы: конвертер RS/KL подключается как антенный коммутатор RS/K с адресом 4 с подключёнными к его входам конвертерами RS/L. Во время анализа приемник перестраивается в диапазоне частот 10 МГц вверх от частоты преобразования конвертера.

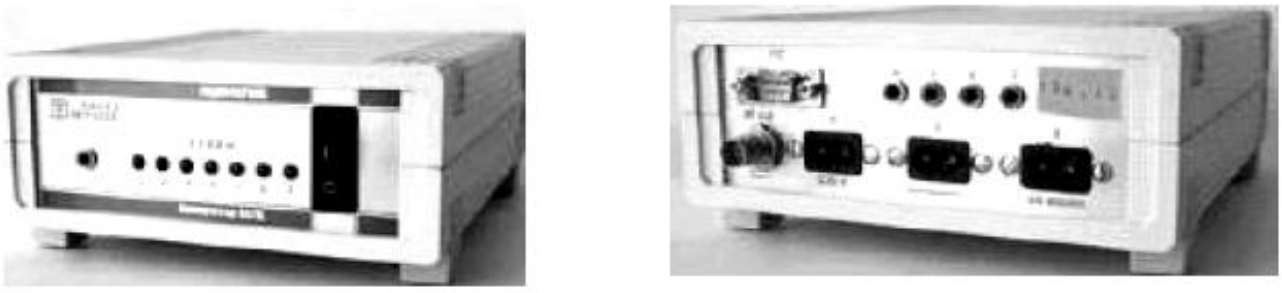


Рисунок 1.58 - Коммутатор-конвертер RS/KL

Программное обеспечение комплексов RS turbo M компании «Радиосервис» в режиме работы с конвертером автоматически пересчитывает и отображает на спектральных панорамах и в списках истинные частоты обнаруженных сигналов.

Изделие МП-3 (рис. 1.59) исключает утечку информации по цепи питания ТСПИ при акустическом воздействии на них и отключенном питающем напряжении.

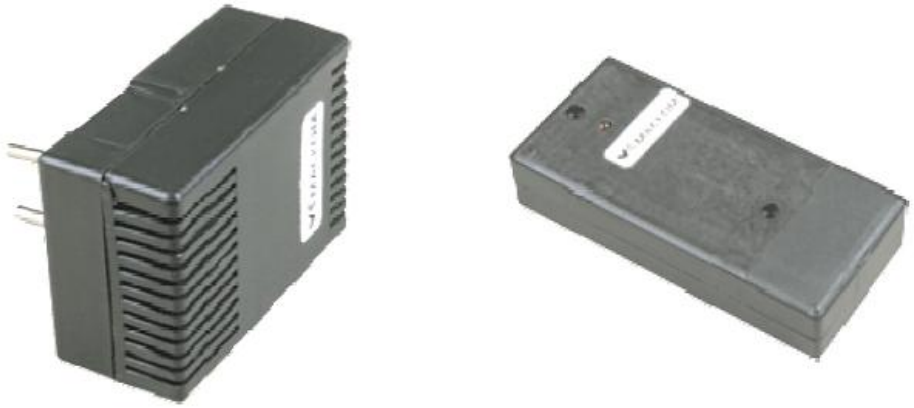


Рисунок 1.59 - Изделия для защиты линий МП-3 и МП-5

В отличие от других изделий, в которых обеспечивается необходимое затухание для информационного сигнала с помощью только какой-либо одной цепи, в «МП-3» реализуется одновременно как разрыв цепи питания с помощью контактов реле, так и затухание с помощью диодно-емкостной цепи, что в сумме обеспечивает внесение затухания на частоте f = 1 кГц более 90 дБ [71].

Интервал регламентных работ определяется лишь вероятностью внештатного замыкания контактов реле. Все стальные неисправности являются обнаруживаемыми.

Изделие МП-5 (рис. 1.59) предназначено для защиты громкоговорителей системы оповещения или однопрограммных приемников от утечки через них акустических сигналов помещения. При отсутствии сигналов оповещения (или сигналов трансляции) громкоговоритель отключен с помощью контактов реле. При появлении штатного сигнала через время t < 5 мс громкоговоритель включается и это состояние удерживается, если t паузы < 10 с. При этих

параметрах изделие МП-5 не влияет на качество сообщения. При отключенном громкоговорителе акустоэлектрический сигнал, измеренный на частоте f = 1 кГц, до попадания в трансляционную линию претерпевает затухание < 90 дБ, чем обеспечивается исключение утечки информации из помещения по цепи трансляции [71].

Изделия МП-1А, МП-1Ц (рис. 1.60) включают в себя как активные средства защиты (АСЗ), так и пассивные средства защиты (ПСЗ).

Рисунок 1.60 - МП-1А и МП-1Ц в российском корпусе и в евророзетке

Изделия МП-1А и МП-1Ц защищают информацию от утечки соответственно в аналоговых и цифровых ТА в режиме ожидания вызова. ПСЗ построены по принципу изделия «Гранит-8», а АСЗ – по принципу изделий «Гранит-11» и «Гранит-12».

Существенным в изделиях МП-1А и МП1-1Ц является то, что, превосходя по всем специальным параметрам указанные изделия типа «Гранит», они на порядок и более выигрывают в массогабаритных характеристиках и потребляемой мощности, что позволяет разместить их внутри телефонных розеток различных типов [71].

Устройство комплексной защиты телефонной линии ПРОТОН (рис.1.61) обеспечивает [71]:

-

Рисунок 1.61 - Устройство комплексной защиты телефонной линии «ПРОТОН» и устройство активной защиты информации BFG-01

- визуальную и звуковую (отключаемую) индикацию при нарушении целостности телефонной линии (короткое замыкание, обрыв);

- цифровую индикацию постоянной составляющей напряжения в телефонной линии во всех режимах работы (режим «АТЛ»);

- работу встроенного вызывного устройства с пороговой регулировкой уровня звука (высокий/низкий);

- развязку телефонного аппарата от телефонной линии при положенной трубке. Питание телефонного аппарата от отдельного стабилизированного внутреннего источника тока (исключает использование резонирующих свойств электромагнитных вызывных устройств);

- шумовую помеху в звуковом диапазоне частот (отключаемую) в телефонную линию при положенной трубке (активизация диктофонов, препятствует прослушиванию помещения);

- автоматическое включение режима минимального тока в телефонной линии без ухудшения качества связи после набора номера абонента;

- обнаружение и противодействие попытке непосредственного прослушивания телефонной линии во время разговора (параллельный аппарат, низкоомные наушники и др.);

- оперативное включение/выключение шумовой помехи, с автоматическим включением режима минимального тока в телефонной линии, в режиме «разговор».

Устройство активной защиты информации BFG (рис. 1.61) предназначено для активной защиты информации от перехвата средствами радиоэлектронного контроля [71].

Устройство представляет собой широкополосный генератор, который создает маскирующий сигнал, затрудняющий прием и расшифровку информации, содержащейся в электромагнитном излучении различных электронных приборов. Устройство имеет выходную мощность, достаточную для защиты информации от утечки не только за счет противодействия перехвату внешних электромагнитных полей средств оргтехники, но и за счет подавления излучений различного рода радиомикрофонов с мощностью излучения до 1 мВт, скрытно размещенных в охраняемом помещении или в непосредственной близости от него.

Прибор делает невозможной двустороннюю связь с помощью радиостанций и сотовых телефонов, существенно снижает вероятность срабатывания радиоуправляемых взрывателей в защищаемом объеме.

Стационарный генератор шума для радиотехнической маскировки и защиты цепей питания ГНОМ-3М (рис. 1.62) предназначен для защиты цепей первичного электропитания и радиотехнической маскировки рабочего помещения [89].

Система контроля функционирования генератора обеспечивает:

- индикацию наличия генерации (свечение светодиода «РАБОТА»);

- выдачу сигнала «АВАРИЯ» в виде уровня напряжения логического «0» на выходе, при этом светодиод «РАБОТА» гаснет.

Рисунок 1.62 - Стационарные шумогенераторы ГНОМ-3М и ГНОМ-3

Генератор шума ГНОМ-3М работает в диапазоне 150 КГц – 1000 МГц, имеет 4 корреляционно не связанных канала (выхода) для подключения к антенным контурам и цепям первичного электропитания, улучшенные весогабаритные характеристики.

Стационарный шумогенератор ГНОМ-3 (рис. 1.62) предназначен для защиты помещений и объектов электронно-вычислительной техники от утечки конфиденциальной информации за счет побочных электромагнитных излучений компьютеров и другой оргтехники. Работает в диапазоне частот шумового сигнала: 10 кГц ... 1 ГГц. Антенны – рамочные, монтируемые в 3-х плоскостях.

Генератор шума ГРОМ – 4 (рис. 1.63) предназначен для защиты от утечки информации за счет побочных электромагнитных излучений средств оргтехники, а также для создания помех устройствам несанкционированного съема информации с телефонных и электрических сетей [89].

Генератор обеспечивает:

- пространственное зашумление в диапазоне 20–1000 МГц, мощность 5 Вт;
- линейное зашумление электросети в диапазоне 0,1–1 МГц, мощность 4 Вт;
- использование эффекта «размывания» спектра акустического сигнала в телефонных линиях;
- независимую работу всех трех режимов.

Устройство защиты телефонных переговоров от прослушивания и записи ПРОКРУСТ ПТЗ-003 (рис. 1.63) предназначено для защиты телефонных переговоров от прослушивания. Подавитель обеспечивает защиту телефонной линии от различных типов телефонных подслушивающих устройств на участке от телефонного аппарата до АТС. Защита осуществляется путем изменения параметров стандартных сигналов. Изделие имеет цифровой дисплей – указатель напряжения на телефонной линии и световой индикатор снятия телефонной трубки [71].

В подавителе предусмотрено три режима подавления, которые могут включаться независимо друг от друга, имеется возможность экстренного отключения всех режимов защиты, подключения диктофона для записи телефонных переговоров. Режим «Уровень» позволяет поднимать напряжение в телефонной линии во время разговора. В режиме «Шум» в линию подается

шумовой сигнал звукового диапазона частот при положенной на рычаг телефонной трубке. В режиме «ВЧ помеха» в линию подается высокочастотный помеховый сигнал вне зависимости от положения телефонной трубки.

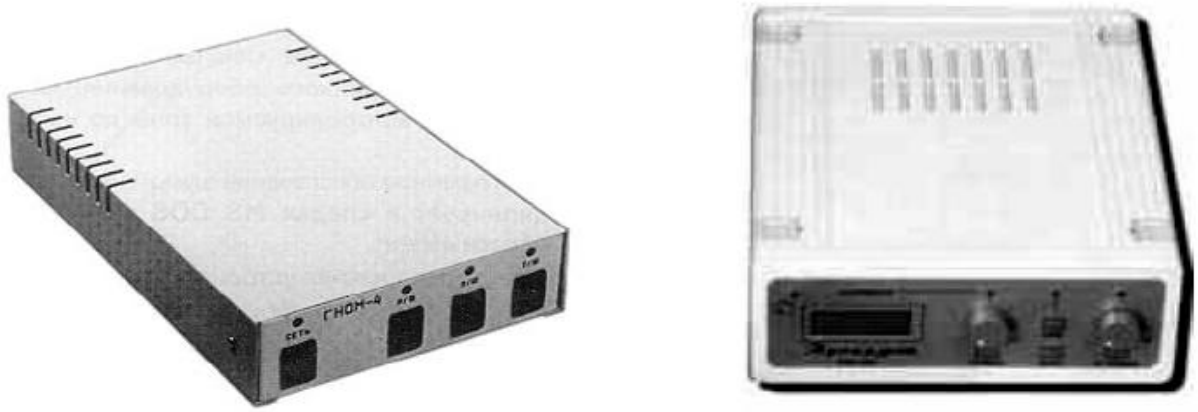


Рисунок 1.63 - Генератор шума ГРОМ-4 и устройство защиты телефонных переговоров ПРОКРУСТ ПТЗ-003

Прибор для защиты телефонных линий RPT-07 (рис. 1.64) предназначен для защиты переговоров по телефонной линии от несанкционированного съема информации. Прибор защищает одну телефонную линию на участке «ТЛФ – аппарат – ГТС» как при поднятой, так и при положенной трубке телефонного аппарата [71].

Рисунок 1.64 - Приборы для защиты телефонных линий RPT-07 и Antifly

Прибор обеспечивает эффективное противодействие:

- радиопередатчикам, включенным в линию последовательно и параллельно (в том числе с бесконтактным съемом и внешним питанием);
- аппаратуре магнитной записи (в т.ч. цифровой), подключаемой к линии контактным или бесконтактным способом;
- параллельным ТА и аналогичной аппаратуре;
- аппаратуре, использующей «ВЧ-навязывание» и «микрофонный эффект»;
- аппаратуре, использующей линию в качестве канала передачи или в качестве источника электропитания.

Прибор имеет выход для подключения головных телефонов или диктофона.

Многофункциональное устройство защиты телефонной линии Antifly (рис. 1.64) предназначено для защиты телефонной линии от различных посторонних вмешательств. Устройство подключается между защищаемым телефонным аппаратом (группой аппаратов) и телефонной линией [71].

Оставаясь практически незаметным для защищаемого аппарата. Устройство обеспечивает следующие защитные функции:

- *Контроль подключения при помощи «мухи»*. При подобном подключении в линии «проскакивают» специфические сигналы (1200 Гц или 2600 Гц). При приеме подобного сигнала устройство, в зависимости от настроек, либо выдает сигнал отбоя для «мухи», либо просто сообщает о попытке подключения при помощи звуковой или световой индикации.

- *«Подавление диктофонов»* – при положенной трубке устройство выдает в линию специальный сигнал, активизирующий (включающий) диктофоны, которые, возможно, подключены к вашей линии. В результате, вместо ваших разговоров диктофоны будут записывать этот сигнал, тратя на это свою пленку.

- *Блокировка незаконного набора.* При попытке подключения и набора номера с линии пользователя при помощи параллельной трубки, устройство включает индикацию и блокирует линию, делая набор невозможным. Под параллельным телефоном понимается любой аппарат, подключенный к линии между устройством и АТС.

- *Контроль параллельного подключения.* Если во время разговора будет снята трубка параллельного телефона, устройство сообщит об этом световой или звуковой индикацией. В устройстве предусмотрена возможность изменения следующих параметров: тип реакции на снятие параллельной трубки, тип реакции на подключение «мухи», чувствительность приемника (3 уровня). Так же имеется возможность регулировки чувствительности датчика параллельного подключения (датчика снятия трубки параллельного телефона). Наличие этих настроек позволяет оптимизировать работу устройства.

Дифференциальный адаптер проводных линий ДАПЛ 031 (рис. 1.65) обеспечивает [71]:

Рис. 1.65. Адаптер проводных линий ДАПЛ 031 и генератор высоковольтных импульсов RPT-02

- обнаружение устройств негласного съема информации, использующие для передачи информации проводные линии;

- оценку воздействия ПЭМИН.

Симметричный вход адаптера позволяет эффективно подавлять внешние помеховые сигналы.

Высокая чувствительность адаптера позволяет обнаруживать:

- передачу сигнала от микрофонов как активных так и пассивных (не имеющих предварительного усилителя).

- наличие «микрофонного эффекта» от средств оргтехники, бытовой РЭА, охранно-пожарной сигнализации и др. в исследуемой линии.

Конструкция измерительных щупов аналогична адаптеру проводных линий и позволяет подсоединять штатные насадки типа «Игла», «Сеть» и «Крокодил».

Подавитель телефонных закладок RPT-02 (рис. 1.65) выполняет следующие функции [71]:

- подавление последовательных и параллельных телефонных радиозакладок;

- отслеживание изменений нагруженности ТЛФ-линии, причиной которого может быть несанкционированное подключение;

- индикация и запоминание пропадания напряжения на линии, причиной которого может быть несанкционированное подключение;

- «выматывание» магнитной ленты диктофонов с акустическим пуском, поставленных на автоматическую запись.

Прибор предназначен для работы как с городской АТС, так и с мини АТС.

Анализатор проводных коммуникаций LBD-50 (рис. 1.66) обеспечивает поиск гальванических подключений к проводным и кабельным линиям любого назначения. Обнаруживает несанкционированные устройства, подключенные к легальным коммуникациям для [71]:

- перехвата информации;

- передачи материалов перехвата;

- обеспечения электропитанием.

Рисунок 1.66 - Анализатор проводных коммуникаций LBD-50

В анализаторе реализован комплекс методов обнаружения, как хорошо известных, так и оригинальных, не имеющих аналогов в мировой практике. Алгоритм обследования, заложенный в анализаторе, исключает срабатывание защитных сторожевых схем в объектах поиска.

1.5.9 Скрытие и защита от утечки информации по акустическому и виброакустическому каналам

Если акустические и виброакустические характеристики защищаемого помещения не соответствуют нормативным требованиям по защите речевой информации, то применяют активные средства защиты. Они представляют собой генераторы акустического и виброакустического маскирующего шума, содержащие аудиоизлучатели, виброизлучатели и пьезоизлучатели.

Наиболее известными генераторами являются «СОНАТА – АВ 1М» и «ШОРОХ» [71].

«СОНАТА – АВ 1М» (рис. 1.67) позволяет перекрыть большинство технических каналов утечки речевой информации, имеет сертификат соответствия требованиям безопасности информации выданный ГТК РФ, гигиенический сертификат соответствия, имеет независимую регулировку уровня помех в каждом канале.

Рисунок 1.67 - Генераторный блок СВАЗ «Соната-АВ»

Стабильность основных характеристик генераторов «Соната-АВ» обеспечивается применением цифровых формирователей шума. Стойкость создаваемой генератором заградительной помехи к различным методам ее

нейтрализации обеспечивается большим периодом используемых последовательностей и шумовой загрузкой регистров формирователя при включении питания.

Правильно установленная и отрегулированная система «Соната-АВ» позволяет нейтрализовать такие виды подслушивания как:

- непосредственное подслушивание в условиях плохой звукоизоляции помещения;
- применение радио- и проводных микрофонов, установленных в полостях стен, в надпотолочном пространстве, вентиляционных коробах и т.п.;
- применение стетоскопов, установленных на стенах (потолках, полах), трубах водо- (тепло-, и газо-) снабжения) и т.п.;
- применение лазерных и микроволновых систем съема аудиоинформации с окон и элементов интерьера.

Все генераторные блоки системы имеют входы удаленного беспроводного управления.

Для построения системы защиты помещения требуются виброизлучатели и пьезоизлучатели. Внешний вид излучателей показан на рис. 1.68.

При наладке устанавливается уровень шумового сигнала, который обеспечивает необходимую степень защиты при минимальном акустическом сигнале помехи в помещении, который практически не влияет на комфортность проведения переговоров.

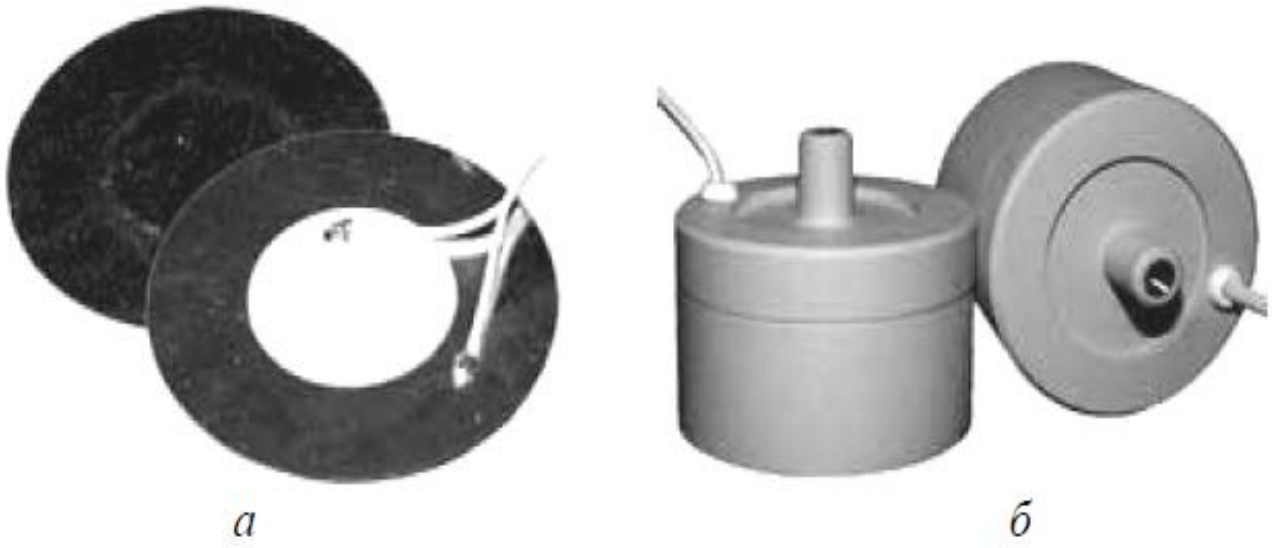


Рисунок 1.68 - Излучатели: а – пьезоизлучателиПИ-45, б – виброизлучатели ВИ-5

Параметры «СОНАТА – АВ 1М» представлены в табл. 1.1.

Таблица 1.1 - Параметры генератора виброакустических помех «СОНАТА – АВ 1М»

Параметр	Значение
1	**2**
Количество независимых каналов	2
Максимальное количество одновременно подключаемых:	
– виброизлучателей большой мощности (ВИ-45)	20 (10+10)
– аудиоизлучателей (АИ-65)	16 (8+8)
– пьезоизлучателей (ПИ-45)	16 (8+8)
Полоса частот вибрационного и акустического шума гарантированной интенсивности	175–5600 Гц
Превышение вибрационного и акустического шума над уровнем речевого сигнала в канале утечки информации	не менее 10 дБ
Наличие ДУ (интерфейс)	есть, (НР-контакт)
Электропитание изделия	сеть ~220 В / 50 Гц
Условия эксплуатации: – температура окружающей среды – относительная влажность воздуха	от 5 до 40°С до 80% при t = 25 °С
Продолжительность непрерывной работы изделия	без ограничения

Виброизлучатель ВИ-45 является специализированным электромеханическим преобразователем повышенной мощности и предназначен для возбуждения шумовых вибраций в массивных конструкциях защищаемого помещения, обеспечивая при этом приемлемый уровень мешающего акустического шума. Конструкция и размеры виброизлучателя и элементов его крепления оптимизированы для установки [71]:

- на ограждающих конструкциях помещения (стенах, потолках, полах, дверях);
- на массивных окнах (как на рамах, так и на стеклах);
- на трубах систем тепло-, водо- и газоснабжения.

Виброизлучатель ПИ-45 (пьезоизлучатель) является специализированным электромеханическим преобразователем малой мощности и предназначен для возбуждения шумовых вибраций в стеклах окон (дверей, офисных перегородок).

Варианты крепления виброизлучателей на строительных конструкциях, трубах и стеклах:

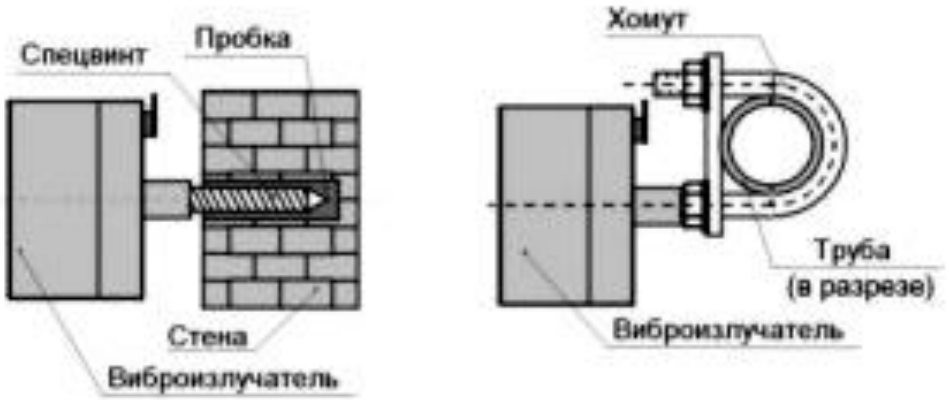


Рисунок 1.69 - Крепление виброизлучателей

Аудиоизлучатель АИ-65 является специализированным электроакустическим преобразователем и предназначен для возбуждения акустического шума.

Конструкция и размеры аудиоизлучателя и элементов его крепления оптимизированы для его установки:

- в надпотолочном пространстве;
- в вентиляционных каналах;
- дверных тамбурах.

Пример подключения нагрузок к генераторному блоку модели 1А приведен на рис. 1.70.

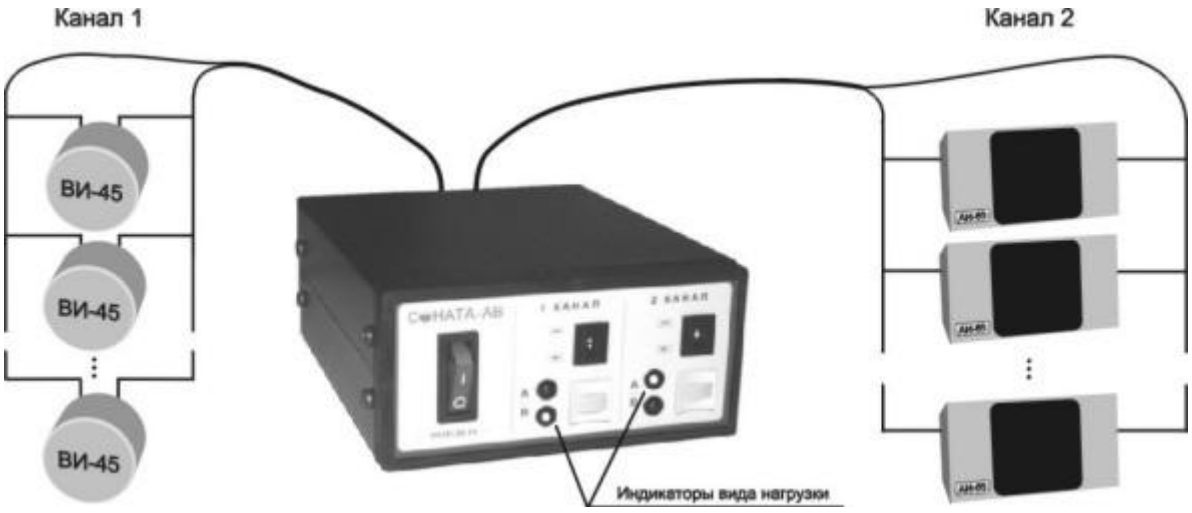


Рисунок 1.70- Подключение нагрузок к генераторному блоку

Мобильный компактный подавитель диктофонов «Мангуст» (рис. 1.71) предназначен для защиты от несанкционированного получения информации при помощи цифровых и кинематических диктофонов [71].

Рисунок 1.71 - Подавитель диктофонов «Мангуст»

Устройство не мешает работе радиоэлектронных устройств (например, средств связи), расположенных вне зоны подавления. В отличии от предыдущих моделей имеет малый вес. «Мангуст» является мобильным устройством, предназначенным для установки прицельной помехи и препятствованию функционированию большинства радиоэлектронных приборов, расположенных в зоне подавления. «Мангуст» воздействует на цепи радиоэлектронных устройств высокочастотным сигналом со специальным видом модуляции, который после навязывания обрабатывается в цепях автоматической регулировки усиления совместно с полезным сигналом, значительно превосходя его по уровню и, соответственно, искажая его. Возможно применение прибора для предотвращения утечки информации при помощи проводных микрофонов, а также малогабаритных передатчиков.

Дальность подавления цифровых диктофонов (типа Samsung SVR-820) до 3 м, дальность подавления аналоговых диктофонов (типа Olympus L-400) – до 4 м.

Другие характеристики:

- сектор излучения в горизонтальной плоскости 60°;
- сектор излучения в вертикальной плоскости 127°;
- дистанционное управление по радиоканалу – 2 пульта;
- вес 4,5 кг;
- питание 12 В – от встроенных аккумуляторов;
- время работы – до 40 мин от полностью заряженных аккумуляторов;
- 220 В – опция;
- зарядное устройство в комплекте;
- размер блока 280×195×60, планшета – 350×265×95**.**

1.5.10 Скрытие речевой информации в телефонных системах с использованием криптографических методов

Применение криптографических методов защиты информации в телефонных системах существенно повышает стойкость и надежность защиты. Очевидно, что в ближайшем будущем криптографические методы защиты информации в телефонных системах станут основными.

Рассмотрим ряд устройств, обеспечивающих криптографическую защиту в телефонных каналах связи [71].

Устройство защиты переговоров в каналах мобильной связи стандарта GSM «Альфа-С» (рис. 1.72) предназначено для защиты речевой информации от несанкционированного доступа. Конструктивно устройство выполнено в виде отдельного блока с гарнитурой и совместимо с мобильными телефонами Siemens.

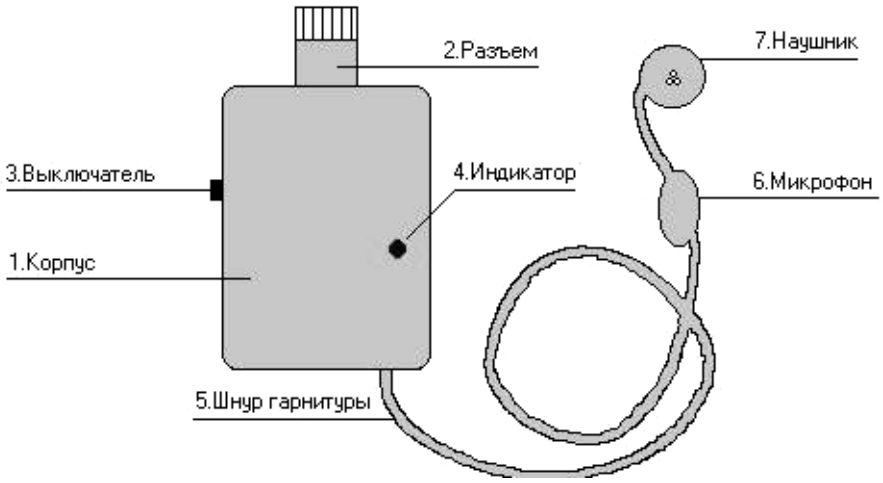


Рисунок 1.72 -Схема устройства «Альфа-С»

Устройство кодирования цифрового потока СКРИПТ – 6401 (рис. 1.73) предназначено для защиты информации, передаваемой по каналам связи, образованным цифровыми потоками Е1 путем канального кодирования.

Рисунок 1.73 - Устройство «Скрипт-6401»

Изделие осуществляет прием линейного сигнала со стороны открытого потока, кодирование информации путем свертки с нелинейным полиномом высокой сложности, формирование и передачу закрытого сигнала в линию, прием линейного сигнала со стороны закрытого потока, раскодирование, формирование и передачу сигнала в направлении открытого потока.

Объектом канального кодирования является поток Е1 с произвольной структурой, в том числе – нефреймированный. Кодированию подвергается вся информация потока Е1, включая информацию сигнализации.

Вид кодирования сигнального уровня (линейный код): HDB3.

На рис. 1.74 приведено типовое включение изделия «Скрипт-6401».

Рисунок 1.74 - Типовое включение «Скрипт-6401»

Два комплекта изделия включаются в разрыв магистрального кабеля потока Е1. Защите подвергается весь участок с учетом оборудования трансляции без ограничения на протяженность участка.

Протяженность кабеля на участках определяется типом кабеля и составляет на каждом участке не менее 270 м для витой пары.

Шифратор телефонных каналов связи, факса, ПК PRAGMA (рис. 1.75) предназначено для гарантированной криптографической защиты телефонных каналов связи, факса, ПК. Приставка «PRAGMA» позволяет защитить от несанкционированного использования документы, базы данных, передаваемые в виде файлов с одного компьютера на другой при помощи модема [71].

Устройство при этом включается вместо обычного модема и работает под управлением стандартного коммуникационного пакета на ПЭВМ в режиме для выделенной линии.

Особенности прибора:

- автономное питание;
- высокая стойкость;
- усиленная ключевая система – 1024 бит;
- возможность оперативной смены мастер-ключа пользователем;
- автономное питание;

Рисунок 1.75 - Приставка «PRAGMA»

- возможность построение конфиденциальной связи в необходимом месте;
- оптимизирован для работы на «дальних» каналах связи (международных, спутниковых);
- симметричное шифрование;
- алгоритм речепреобразования – CELP 4800 бод;
- защита факсимильных документов путем шифрования передаваемого изображения, в защищенный факсимильный документ добавляется «шапка», внешний вид которой может задавать сам пользователь;
- защита факсимильных документов происходит автоматически, не требуя вмешательства пользователя;
- защита межкомпьютерного обмена данными;
- система открытого распределения ключей Диффи-Хеллмана (1024 бит) создает уникальный ключ для каждого сеанса связи и исключает необходимость ввода сеансовых ключей пользователем;
- система проверки подлинности, исключающая возможность вмешательства «третьей» стороны (атаки вида «человек посредине»), даже при наличии подобного устройства. Решается это применением алгоритмов «защищенные переговоры о согласовании ключа»;
- возможность смены ключевых и др. параметров работы устройства самим пользователем;
- возможность оперативной смены ключевых параметров (предусмотрен инжектор ключей, позволяющий менять ключевые параметры устройства). При этом осуществляется проверка на целостность ключевых параметров, предотвращающая несанкционированное навязывание параметров ключевой системы;
- исключение возможности влияния производителя устройства на систему защиты, организуемой пользователем.

«PRAGMA» представляет собой шифратор нового поколения, позволяющий создавать конфиденциальные сети связи с защитой всего канала, от одного шифратора до другого, предотвращает прослушивание речевых переговоров, перехват факсимильных документов и передаваемых данных при

межкомпьютерном обмене. Максимальное количество абонентов сети неограниченно [71].

Качество восстановленного (синтезированного) сигнала практически не отличается, а во многих случаях выше обычного открытого.

«PRAGMA» выполнен в виде приставки к телефонному (факсимильному) аппарату и подключается между телефонной линией и телефоном. Для передачи данных устройство соединяется с компьютером по последовательному коммуникационному порту (COM).

При защите факсимильных документов шифруется само изображение передаваемое на скоростях 2400–9600 бит/с. При этом сигналы в телефонной линии не отличаются от обычной факсимильной передачи.

Для построения системы защищенной связи необходимы как минимум два устройства «PRAGMA». Приставки включаются в разрыв между телефонным (факсимильным) аппаратом и телефонной линией у каждого абонента и обеспечивают защиту от прослушивания в открытом канале связи на участке от одного устройства до другого.

При включении питания осуществляется самотестирование устройства и переход в режим ожидания. О правильной работе в режиме ожидания свидетельствует поочередное включение/выключение индикаторов режимов работы. В таком состоянии (а так же при выключенном питании) приставка «прозрачна» для всех операций с телефонным (факсимильным) аппаратом и не мешает обычной работе пользователя.

Перевод устройства в режим защиты переговоров должен производиться после установления связи между абонентами и может осуществляться несколькими способами:

- нажатием кнопки;
- набором определенной комбинации цифр (символов) с клавиатуры телефонного аппарата в режиме тонального набора;
- устройство может включаться автоматически при обнаружении служебных посылок со стороны второго абонента.

Переход в режим открытой связи (ожидания) осуществляется нажатием соответствующей кнопки или автоматически, при переключении в открытый режим противоположного абонента. Если ложится трубка телефонного аппарата, приставка отключается и возвращается в режим ожидания.

Защита факсимильных документов осуществляется без вмешательства пользователя. Устройство включается при обнаружении начала факсимильной процедуры, шифрует передаваемый документ (дешифрует принимаемый) при наличии такой же приставки (с таким же ключом) с противоположной стороны и возвращается в режим ожидания.

Защищенный документ помечается специальной строкой в начале каждой страницы.

Предусмотрена возможность блокирования приема и/или передачи факсимильного документа в незащищенном режиме.

Устройство защиты речевой и факсимильной информации в открытых каналах связи ALT-4132M (рис. 1.76) предназначено для предотвращения прослушивания речевых переговоров, перехвата факсимильных документов [71].

Рисунок 1.76 - Устройство «ALT-4132M»

ALT-4132M выполнен в виде приставки к телефонному (факсимильному) аппарату и подключается между телефонной линией и телефоном.

Защита речевой информации осуществляется путем вокодерного преобразования и шифрования по алгоритму ГОСТ28149-89 с высокой стойкостью к вскрытию.

Аппарат может эксплуатироваться с факс-машинами и факс-модемами группы 3 (ISO, G3).

Обеспечивается гальваническая развязка с линией и телефонным (факсимильным) аппаратом.

Обеспечивается передача и прием факсимильных документов без снижения скорости по сравнению с открытой передачей согласно рекомендациям ITU.T (T.30, T.4, V.27ter-2400, V27ter-4800, V.29-7200, V.29-9600).

Сигналы в линии при работе устройства в режиме защиты факсимильных сообщений не отличаются от сигналов стандартной факсимильной процедуры.

В устройстве защиты переговоров УКС-001 (рис. 1.77) реализован абонентский метод шифрования в каналах сотовой связи стандарта GSM 900/1800 на базе созданного криптографического устройства конфиденциальной связи УКС-001 [71].

УКС-001 совместно с подключенным к нему мобильным телефоном Ericsson-R520m обеспечивает проведение сеансов защищённых переговоров по каналу передачи данных.

Криптографическая стойкость защищённого УКС-001 канала связи подтверждена государственной экспертизой.

Основные свойства устройства:

- время непрерывной работы в режиме секретной связи не менее 4 ч, в режиме ожидания – не менее 100 ч;

- размер секретного ключа шифрования 256 бит;

- загрузка секретных ключей в память УКС-001 на каждые 30 дней переговоров производится в центре сопровождения или самим пользователем 1 раз в месяц;

- для повышения степени защищённости пользователей устройство автоматически производит ежедневную смену секретных ключей;

- отсутствует возможность использования УКС-001 другим лицом в случае его утери.

Рисунок 1.77 - Устройство «УКС-001»

Устройство маскирования телефонных сообщений (УМТС) в каналах GSM связи РЕЗЕДА (рис.1.78) предназначено для защиты телефонных сообщений, передаваемых между мобильными радиотелефонами сотовых сетей стандарта GSM, от несанкционированного доступа (НСД) к их содержимому [71].

Защита телефонных сообщений от НСД обеспечивается путем изменения по определенному, неизвестному для потенциального злоумышленника, правилу спектра передаваемого сигнала.

Такое техническое решение исключает оперативный перехват телефонных переговоров, т.к. для восстановления телефонных сообщений требует применения специальной аппаратуры и осуществления временных затрат подготовленных специалистов порядка 150 ч.

УМСТ размещается в специально изготовленном металлическом контейнере размером 43×15×11 мм, с одной стороны к которому подключена микротелефонная гарнитура, а с другой стороны – кабель с разъемом, с помощью которого УМСТ штатно подключается к радиотелефону. Для питания УМСТ используется аккумуляторная батарея радиотелефона.

Рисунок 1.78 - Устройство «РЕЗЕДА»

Устройство защиты речевой информации в открытых каналах связи ОРЕХ-2 (рис. 1.79) предназначено для организации засекречивающей связи с высокой степенью защищенности от несанкционированного восстановления информации, передаваемой по коммутируемым или выделенным каналам связи с 2-х проводным абонентским окончанием [71].

Рисунок 1.79 - Устройство «ОРЕХ-2»

Защита речевой информации осуществляется методом частотновременного скремблирования. Устройство обеспечивает уникальный ключ на каждый сеанс

связи и возможность аутентификации с использованием пароля, вводимого с телефонного аппарата, управление одной кнопкой. Использует систему открытого распределения ключей Диффи-Хеллмана.

Закрытие речевой информации достигается следующими методами: временных перестановок; инверсии спектра сигнала; преобразования временного масштаба, разрушающего непрерывность речевого сигнала.

Стойкость защиты информации к несанкционированному вскрытию обеспечивается трехуровневой ключевой системой, включающей в себя: пароль – предназначен для идентификации абонентов, входящих в связь, вводится с клавиатуры телефонного аппарата, подключенного к приставке, содержит четыре цифры (используется при необходимости); мастер-ключ разрядностью 128 бит – для заказываемой партии телефонных приставок (размещается в постоянном запоминающем устройстве); сеансовый ключ – генерируется физическим датчиком случайный чисел и имеет разрядность 128 бит.

Обмен сеансовыми ключами в приставке реализован по методу открытого распределения ключей с генерацией разовых ключей для каждого сеанса связи. Ключ формируется от физического датчика случайных чисел и является уникальным для каждого сеанса связи. Сформированный ключ является достаточным для установления надежной защиты, однако, дополнительно предусмотрена возможность аутентификации с помощью пароля, который может вводиться пользователем с клавиатуры телефонного аппарата. Пароль может использоваться, например, для организации иерархической структуры, когда пользователю высшего звена известны все пароли структуры, и он имеет возможность связываться со всеми звеньями, а пользователь низшего звена, зная лишь свой пароль, работает только на своем уровне.

1.5.11 Защита информации с ограниченным доступом от несанкционированного доступа в информационных, телекоммуникационных и информационно-телекоммуникационных системах

1.5.11.1 Secret Net 5.0

Secret Net 5.0 – это система защиты информации с ограниченным доступом от несанкционированного доступа нового поколения, которая реализует требования руководящих документов по защите информации и функционирует под управлением современных ОС MS Windows 2000, Windows XP и Windows 2003. Существует в автономном и сетевом вариантах [71].

За счёт интеграции собственных защитных механизмов с механизмами управления сетевой инфраструктуры защищаемой сети Secret Net 5.0 повышает защищенность всей автоматизированной информационной системы в целом и при этом [90]:

- обеспечивает централизованное управление настройками политики безопасности;

- работает совместно с ОС Windows, расширяя, дополняя и усиливая стандартные механизмы защиты;

- осуществляет мониторинг и аудит политики безопасности в режиме реального времени;

- позволяет оперативно реагировать на события НСД;

- поддерживает терминальный режим работы пользователей с рабочей станцией.

Структура Secret Net 5.0 показана на рис. 1.80.

Рисунок 1.80 - Структура Secret Net 5.0

Интеграция системы управления Secret Net 5.0 со штатным механизмами управления информационной системой позволяет избежать постоянно возникающих проблем синхронизации данных между ИС и выделенным сервером настроек, который имелся в предыдущих версиях системы и часто присутствует в аналогичных системах защиты.

Система обеспечивает:

- оперативное реагирование на действия злоумышленников;
- централизованный просмотр событий безопасности;
- контроль вывода конфиденциальной информации на внешние носители;
- аппаратную идентификацию пользователей;
- централизованное управление;
- контроль целостности файлов;
- разграничение доступа к устройствам (CD\DVD, USB, Wi-Fi и т.д.).

Secret Net 5.0 (сетевой вариант) содержит следующие компоненты:

- клиент Secret Net 5.0;

- сервер безопасности Secret Net 5.0;
- программу оперативного управления, мониторинга и аудита («Монитор»);
- модификатор схемы Active Directory.

Клиент

Клиент Secret Net 5.0 следит за соблюдением настроенной политики безопасности на рабочих станциях и серверах, обеспечивает регистрацию событий безопасности и передачу журналов на Сервер Безопасности, а также приём от него оперативных команд и их выполнение.

Сервер безопасности

Сервер безопасности производит сбор журналов от зарегистрированных на нем агентов, накапливает полученную информацию в базе данных и обеспечивает выдачу команд оперативного управления клиентам (например, блокировку рабочей станции при выявлении попытки НСД).

Программа оперативного управления, мониторинга и аудита («Монитор»)

Монитор является программой, которая отображает администратору оперативную информацию от Сервера Безопасности о состоянии рабочих станций и дает возможность отслеживать:

- какие компьютеры сети в данный момент включены;
- какие пользователи на них работают (как локально, так и в терминальном режиме).

«Монитор» в режиме реального времени отображает оперативную информацию о происходящих событиях НСД, позволяет осуществлять просмотр журналов всех рабочих станций, а также выдавать на защищаемые рабочие станции команды оперативного управления.

Модификатор схемы Active Directory

Модификатор схемы Active Directory (AD) используется для подготовки схемы ОС Windows к развертыванию Secret Net 5.0. Так как в качестве хранилища информации о настройках безопасности Secret Net 5.0 использует AD, данный модуль создаёт новые объекты и изменяет параметры существующих. Программы управления объектами и параметрами групповых политик, входящие в состав этого модуля, обеспечивают управление параметрами работы доменных пользователей и применение централизованных настроек безопасности Secret Net 5.0.

Управление системой Secret Net 5.0

Система централизованного управления

В качестве хранилища информации в системе централизованного управления используется Active Directory (AD). Для нужд централизованного управления Secret Net 5.0 схема Active Directory расширяется – создаются новые объекты и изменяются параметры существующих.

Для выполнения этих действий используется специальный модуль изменения схемы AD, который устанавливается и запускается на контроллере домена при установке системы централизованного управления. Для приведения параметров работы защитных средств компьютера в соответствие настройкам безопасности Secret Net 5.0, задаваемым с помощью групповых политик,

используется агент Secret Net 5.0, установленный на каждом сервере или рабочей станции защищаемой сети.

Столь тесная интеграция системы управления с Active Directory позволяет легко использовать Secret Net 5.0 для организации защиты сети, использующей многодоменную структуру.

Оперативный мониторинг и аудит

В Secret Net 5.0 предусмотрена функция оперативного мониторинга и аудита безопасности информационной системы предприятия, которая позволяет решать такие задачи, как:

- оперативный контроль состояния автоматизированной системы предприятия (получение информация о состоянии рабочих станций и о работающих на них пользователях);
- централизованный сбор журналов с возможностью оперативного просмотра в любой момент времени, а также хранение и архивирование журналов;
- оповещение администратора о событиях НСД в режиме реального времени;
- оперативное реагирование на события НСД – выключение, перезагрузка или блокировка контролируемых компьютеров;
- ведение журнала НСД.

Система оперативного управления имеет свою базу данных, в которой хранится вся информация, связанная с работой сервера по обеспечению взаимодействия компонентов, а также журналы, поступающие от агентов.

В качестве базы данных используется СУБД Oracle 9i.

Мониторинг

С помощью программы мониторинга администратор может управлять сбором журналов с рабочих станций. Предусмотрено два варианта. Первый – сервер оперативного управления собирает журналы по команде администратора. Второй – администратор составляет расписание и передает его серверу, далее сервер собирает журналы в соответствии с этим расписанием.

Также предусмотрена возможность создать удобный для администратора вид представления сети – так называемый «срез» (например, по отделам, по территориальному размещению и т.п.). В случае крупной распределённой сети эта функция делегируется другим администраторам для управления выделенными им сегментами сети.

Аудит

Программа работы с журналами устанавливается на рабочем месте сотрудника, уполномоченного проводить аудит системы защиты. Если функции мониторинга и аудита совмещает один сотрудник, программа устанавливается на том же компьютере, который является рабочим местом администратора оперативного управления.

В системе Secret Net 5.0 для проведения аудита используются 4 журнала:

- журнал приложений;
- журнал безопасности;
- журнал системы;

- журнал Secret Net.

Первые три из перечисленных журналов – штатные, входящие в состав средств операционной системы. В журнале Secret Net хранятся сведения о событиях, происходящих в системе Secret Net 5.0.

Журналы ведутся на каждом защищаемом компьютере сети и хранятся в его локальной базе данных. Сбор журналов осуществляется по команде аудитора или по расписанию.

Программа работы с журналами позволяет аудитору просматривать записи журналов и тем самым отслеживать действия пользователей, связанные с безопасностью автоматизированной информационной системы предприятия.

В программе управления журналами предусмотрена настраиваемая выборка записей, используя которую аудитор может просматривать не весь журнал целиком, а только часть записей, удовлетворяющих определенным критериям. Это значительно ускоряет и упрощает работу, связанную с поиском и анализом событий.

С помощью программы работы с журналами аудитор может выдавать команды серверу на архивацию журналов, а также на восстановление журналов из архива. Предусмотрена возможность просмотра архивов, а также сохранения журнала в файл для последующей передачи и анализа записей вне системы Secret Net 5.0.

Защитные механизмы

Усиленная идентификация и аутентификация пользователей

Система Secret Net 5.0 совместно с ОС Windows обеспечивает усиленную идентификацию и аутентификацию пользователя с помощью средств аппаратной поддержки при его входе в систему, а также позволяет существенно снизить риски того, что пользователь загрузит компьютер с отчуждаемых внешних носителей и получит доступ к важной информации в обход системы защиты.

В качестве аппаратной поддержки система Secret Net 5.0 использует: программно-аппаратный комплекс «Соболь» и Secret Net Touch Memory Card. Плату аппаратной поддержки невозможно обойти средствами BIOS. Если в течение определённого времени после включения питания на плату не было передано управление, она блокирует работу всей системы.

Полномочное управление доступом

Каждому информационному ресурсу назначается один их трёх уровней конфиденциальности: «Не конфиденциально», «Конфиденциально», «Строго конфиденциально», а каждому пользователю – уровень допуска. Доступ осуществляется по результатам сравнения уровня допуска с категорией конфиденциальности информации.

Разграничение доступа к устройствам

Функция обеспечивает разграничение доступа к устройствам с целью предотвращения несанкционированного копирования информации с защищаемого компьютера. Существует возможность запретить, либо разрешить пользователям работу с любыми портами/устройствами.

Разграничивается доступ к следующим портам/устройствам:

- последовательным и параллельным портам;

- сменным, логическим и оптическим дискам;
- USB – портам.

Также поддерживается контроль подключения устройств на шинах USB, PCMCIA, IEEE1394 по типу и серийному номеру, права доступа на эти устройства задаются не только для отдельных пользователей, но и для групп пользователей.

Существует возможность запретить использование сетевых интерфейсов – Ethernet, 1394 FireWire, Bluetooth, IrDA, WiFi.

Замкнутая программная среда

Для каждого пользователя компьютера формируется определённый перечень программ, разрешенных для запуска. Он может быть задан как индивидуально для каждого пользователя, так и определен на уровне групп пользователей. Применение этого режима позволяет исключить распространение вирусов, «червей» и шпионского ПО, а также использования ПК в качестве игровой приставки.

Контроль целостности

Используется для слежения за неизменностью контролируемых объектов с целью защиты их от модификации. Контроль проводится в автоматическом режиме в соответствии с некоторым заданным расписанием.

Объектами контроля могут быть файлы, каталоги, элементы системного реестра и секторы дисков. Каждый тип объектов имеет свой набор контролируемых параметров. Так, файлы могут контролироваться на целостность содержимого, прав доступа, атрибутов, а также на их существование, т.е. на наличие файлов по заданному пути. При обнаружении несоответствия предусмотрены следующие варианты реакции на возникающие ситуации нарушения целостности:

- регистрация события в журнале Secret Net;
- блокировка компьютера;
- восстановление повреждённой/модифицированной информации;
- отклонение или принятие изменений.

Гарантированное уничтожение данных

Уничтожение достигается путем записи случайной последовательности на место удаленной информации в освобождаемую область диска. Для большей надежности может быть выполнено до 10 циклов (проходов) затирания.

Контроль аппаратной конфигурации компьютера

Осуществляет своевременное обнаружение изменений в аппаратной конфигурации компьютера и реагирования на эти изменения.

Предусмотрено два вида реакций:

- регистрация события в журнале Secret Net;
- блокировка компьютера.

Контроль печати конфиденциальной информации

Администратор безопасности имеет возможность запретить вывод конфиденциальной информации на печать, либо разрешить эту операцию некоторым пользователям, при этом распечатанные документы могут автоматически маркироваться в соответствии с правилами оформления

документов. Также сам факт печати (или попытки несанкционированного вывода на печать) отображается в журнале защиты Secret Net 5.0.

Регистрация событий

Система Secret Net 5.0 регистрирует все события, происходящие на компьютере: включение\выключение компьютера, вход\выход пользователей, события НСД, запуск приложений, обращения к конфиденциальной информации, контроль вывода конфиденциальной информации на печать и отчуждаемые носители и т.п.

Функциональный самоконтроль подсистем

Самоконтроль производится перед входом пользователя в систему и предназначен для обеспечения гарантии того, что к моменту завершения загрузки ОС все ключевые компоненты Secret Net 5.0 загружены и функционируют.

Импорт и экспорт параметров

В Secret Net 5.0 реализована возможность экспорта и импорта различных параметров системы. После проверки корректности работы защитных механизмов на компьютере, принимаемом за эталонный, выполняется экспорт значений параметров в файл. Далее значения импортируются на необходимое количество компьютеров.

1.5.11.2 Электронный замок «СОБОЛЬ»

Среди средств так называемых AAA (authentication, authorization, administration – аутентификация, авторизация, администрирование) важное место занимают программно-аппаратные инструменты контроля доступа к компьютерам – электронные замки, устройства ввода идентификационных признаков (УВИП) и соответствующее программное обеспечение (ПО).

В этих средствах контроля доступа к компьютерам идентификация и аутентификация, а также ряд других защитных функций, выполняются с помощью электронного замка и УВИП до загрузки ОС [71].

По способу считывания современные УВИП подразделяются на контактные, дистанционные и комбинированные.

Контактное считывание идентификационных признаков осуществляется непосредственным взаимодействием идентификатора и считывателя.

При бесконтактном способе считывания идентификатор может располагаться на некотором расстоянии от считывателя, а сам процесс считывания осуществляется радиочастотным или инфракрасным методом.

УВИП могут быть электронными, биометрическими и комбинированными.

Электронные УВИП содержат микросхему памяти идентификационного признака.

Примером электронного замка может служить устройство «СОБОЛЬ» (рис. 1.81) [71].

Рисунок 1.81 - Электронный замок «Соболь-PCI»

Назначение

Применяется для защиты ресурсов компьютера от несанкционированного доступа.

Применение

Электронный замок «Соболь» может применяться как устройство, обеспечивающее защиту автономного компьютера, а также рабочей станции или сервера, входящих в состав локальной вычислительной сети.

Электронный замок «Соболь» обладает следующими возможностями:

- идентификация и аутентификация пользователей;
- регистрация попыток доступа к ПЭВМ;
- запрет загрузки ОС со съемных носителей;
- контроль целостности программной среды.

Возможности по идентификации и аутентификации пользователей, а также регистрация попыток доступа к ПЭВМ не зависят от типа использующейся ОС.

Идентификация и аутентификация пользователей

Каждый пользователь компьютера регистрируется в системе электронный замок «Соболь», установленной на данном компьютере. Регистрация пользователя осуществляется администратором и состоит в определении имени регистрируемого пользователя, присвоении ему персонального идентификатора и назначении пароля.

Действие электронного замка «Соболь» состоит в проверке персонального идентификатора и пароля пользователя при попытке входа в систему. В случае попытки входа в систему не зарегистрированного пользователя электронный

замок «Соболь» регистрирует попытку НСД и осуществляется аппаратная блокировка до 4-х устройств (например: FDD, CD-ROM, ZIP, LPT, SCSI-порты).

В электронном замке «Соболь» используются идентификаторы Touch Memory фирмы Dallas Semiconductor. Загрузка операционной системы с жесткого диска осуществляется только после предъявления зарегистрированного идентификатора. Служебная информация о регистрации пользователя (имя, номер присвоенного персонального идентификатора и т.д.) хранится в энергонезависимой памяти электронного замка.

Регистрация попыток доступа к ПЭВМ

Электронный замок «Соболь» осуществляет ведение системного журнала, записи которого хранятся в специальной энергонезависимой памяти. Электронный замок «Соболь» фиксирует в системном журнале вход пользователей, попытки входа, попытки НСД и другие события, связанные с безопасностью системы.

В системном журнале хранится следующая информация: дата и время события, имя пользователя и информация о типе события, например:

- факт входа пользователя;
- введение неправильного пароля;
- предъявление не зарегистрированного идентификатора пользователя;
- превышение числа попыток входа в систему;
- другие события.

Таким образом, электронный замок «Соболь» предоставляет информацию администратору о всех попытках доступа к ПЭВМ.

Контроль целостности программной среды и запрет загрузки со съемных носителей

Подсистема контроля целостности расширяет возможности электронного замка «Соболь». Контроль целостности системных областей дисков и наиболее критичных файлов производится по алгоритму в режиме имитовставки. Администратор имеет возможность задать режим работы электронного замка, при котором будет блокирован вход пользователей в систему при нарушении целостности контролируемых файлов.

Подсистема запрета загрузки с гибкого диска и CD ROM диска обеспечивает запрет загрузки операционной системы с этих съемных носителей для всех пользователей компьютера, кроме администратора. Администратор может разрешить отдельным пользователям компьютера выполнять загрузку операционной системы со съемных носителей.

Подсистемы контроля целостности и подсистемы запрета загрузки со съемных носителей функционируют под управлением следующих ОС:

MS DOS версий 5.0-6.22 (только ЭЗ «Соболь» для стандарта ISA); ОС семейства Windows’9x (FAT12, FAT16 или FAT32); Windows NT версий 3.51 и 4.0 с файловой системой NTFS; Windows 2000 с файловой системой NTFS (только «Соболь-PCI»); UNIX FreeBCD (только «Соболь-PCI»).

Возможности по администрированию

Для настройки электронного замка «Соболь» администратор имеет возможность:

- определять минимальную длину пароля пользователя;
- определять предельное число неудачных входов пользователя;
- добавлять и удалять пользователей;
- блокировать работу пользователя на компьютере;
- создавать резервные копии персональных идентификаторов.

Использование

Электронный замок «Соболь» может применяться в составе системы защиты информации Secret Net для генерации ключей шифрования и электронно-цифровой подписи. Кроме того, при использовании ЭЗ «Соболь» в составе СЗИ Secret Net обеспечивается единое централизованное управление его возможностями. С помощью подсистемы управления Secret Net администратор безопасности имеет возможность управлять статусом персональных идентификаторов сотрудников: присваивать электронные идентификаторы, временно блокировать, делать их недействительными, что позволяет управлять доступом сотрудников к компьютерам автоматизированной системы организации.

1.5.11.3 USB-ключ

Основное технологическое отличие USB-ключа от смарт-карты заключается в том, что хранимая в памяти USB-ключа информация не привязана жестко к ячейкам памяти, а располагается в специальной файловой системе. Поэтому один и тот же ключ можно использовать для разных целей: для входа в компьютер, авторизации электронной почты, создания канала виртуальной частной сети (VPN – virtual private network) и многого другого. Таким образом, с помощью одного аппаратного ключа можно комплексно решить задачу идентификации пользователя для всего комплекса офисного программного обеспечения. При этом человек не должен знать пароли и ключи шифрования для всех приложений, достаточно одного пароля для работы с ключом [71].

Для повышения надежности защиты некоторые аппаратные ключи выполнены в герметичном, влагостойком и пыленепроницаемом корпусе, что гарантирует защищенность данных от многих внешних воздействий. При разгерметизации корпуса информация из памяти ключа стирается. Это сделано для того, чтобы блокировать копирование или подделку ключа и обеспечить достаточно надежное хранение информации внутри аппаратного идентификатора при более жестких требованиях к его конструктиву. Реализовать те же самые требования для всего компьютера значительно сложнее.

Назначение USB-ключа [71]*:*

- строгая двухфакторная аутентификация пользователей при доступе к защищённым ресурсам (компьютерам, сетям, приложениям);
- аппаратное выполнение криптографических операций в доверенной среде (в электронном ключе: генерация ключей шифрования, симметричное и асимметричное шифрование, вычисление хэш-функции, выработка ЭЦП);

- безопасное хранение криптографических ключей, профилей пользователей, настроек приложений, цифровых сертификатов и пр. в энергонезависимой памяти ключа;

- поддержка большинством современных операционных систем, бизнес приложений и продуктов по информационной безопасности в качестве средства аутентификации и авторизации.

Возможности применения USB-ключа:

- строгая аутентификация пользователей при доступе к серверам, базам данных, разделам веб сайтов;

- безопасное хранение секретной информации: паролей, ключей ЭЦП и шифрования, цифровых сертификатов;

- защита электронной почты (цифровая подпись и шифрование, доступ);

- защита компьютеров;

- защита сетей, VPN;

- клиент-банк, домашний банк;

- электронная торговля.

Преимущества

USB-ключ, может использоваться в любых приложениях для замены парольной защиты на более надежную двухфакторную аутентификацию (когда пользователь имеет нечто – USB-ключ, и знает нечто – PIN код).

USB-ключ обеспечивает:

- строгую аутентификацию пользователей за счет использования криптографических методов;

- безопасное хранение ключей шифрования и ЭЦП (электронной цифровой подписи), а также цифровых сертификатов для доступа к защищенным корпоративным сетям и информационным ресурсам;

- мобильность для пользователя и возможность работы в «не доверенной среде» (например, с чужого компьютера) – за счет того, что ключи шифрования и ЭЦП генерируются в памяти USB-ключ аппаратно и не могут быть перехвачены;

- безопасное использование – воспользоваться им может только его владелец, знающий PIN-код;

- реализацию как российских, так и западных стандартов шифрования и ЭЦП;

- удобство работы – USB-ключ выполнен в виде брелока со световой индикацией режимов работы и напрямую подключается к USB-портам, которыми сейчас оснащаются 100% компьютеров, не требует специальных считывателей, блоков питания, проводов и т.п.;

- использование одного ключа для решения множества различных задач – входа в компьютер, входа в сеть, защиты канала, шифрования информации, ЭЦП, безопасного доступа к защищённым разделам Web-сайтов, информационных порталов и т.п.

USB-ключ имеет (рис. 1.82):

- микросхему (1);

- защищенный микроконтроллер (2);

- разъем USB (3);

- световой индикатор режимов работы (4);
- герметичный полупрозрачный пластиковый корпус.

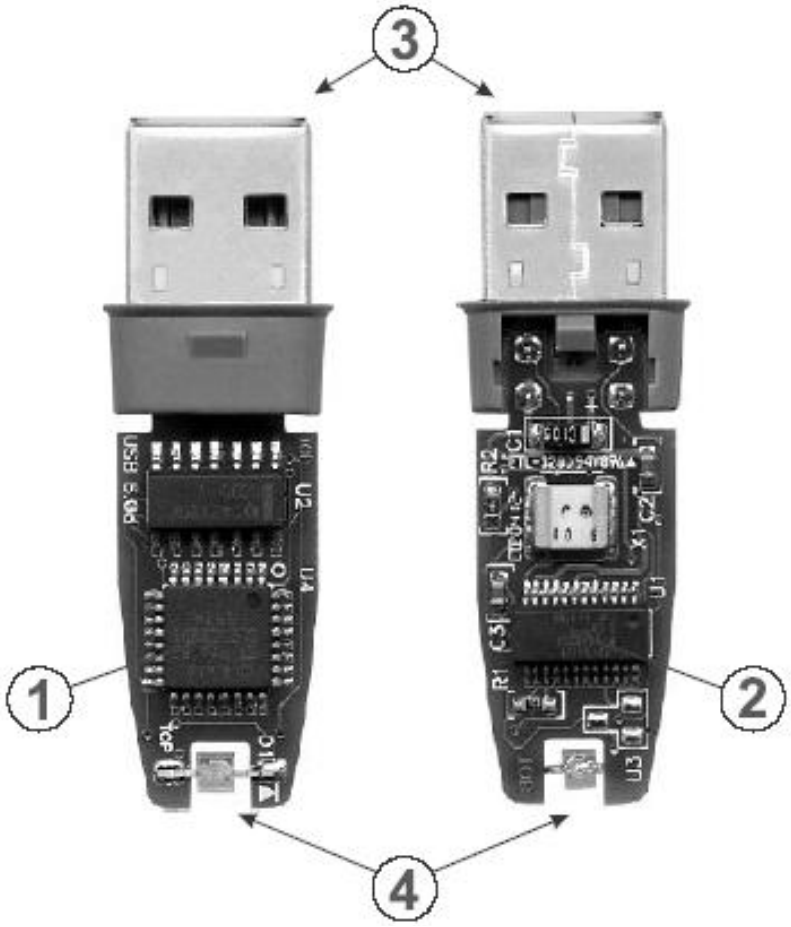


Рисунок 1.82 - USB-ключ

Микроконтроллер в составе USB-ключа обеспечивает:
- коммуникационные функции (поддержку протокола USB);
- хранение микрокода для управления протоколом передачи (firmware).

В состав микросхемы входят:
- 16-ти битный центральный процессор с набором инструкций;
- память только для чтения (ROM, Read Only Memory), содержащая операционную систему;
- оперативная память (RAM, Random Access Memory), предназначенная для использования операционной системой;
- электрически стираемая программируемая память только для чтения (EEPROM, Electrically Erasable Programable Read Only Memory), предназначенная для хранения пользовательских данных;
- аппаратный генератор случайных чисел;
- криптопроцессор для ускорения выполнения криптографических операций.

1.5.11.4 Считыватели «Proximity»

Технология Proximity прочно завоевала ведущее место в профессиональных системах управления доступом, потеснив магнитные и Wiegand считыватели и практически полностью вытеснив Touch memory [71].

Устройства ввода идентификационных признаков на базе идентификаторов Proximity (от английского слова proximity – близость, соседство) относится к классу электронных бесконтактных радиочастотных устройств.

Они выпускаются в виде карточек, ключей, брелоков и т.п. Каждый из них имеет собственный уникальный серийный номер. Основными составляющими устройств являются интегральная микросхема для связи со считывателем и встроенная антенна. В составе микросхемы находятся приемопередатчик и запоминающее устройство, хранящее идентификационный код и другие данные. Внутри Proximity может быть встроена литиевая батарейка (активные идентификаторы). Активные идентификаторы могут считывать информацию на расстоянии нескольких метров. Расстояние считывания пассивными идентификаторами (не имеющих батарейки) составляет десятки сантиметров.
Устройство считывания постоянно излучает радиосигнал, который принимается антенной и передается на микросхему. За счет принятой энергии идентификатор излучает идентификационные данные, принимаемые считывателем.

Рассмотрим принципы работы считывателей «Parsec» [71].

Считыватели Proximity в своей работе опираются на широко известные физические принципы. Правда, того же нельзя сказать об алгоритмах обработки сигналов в схеме считывателя, что обычно и составляет «ноу хау» производителей. Рис. 1.83 поясняет взаимодействие карты и считывателя в процессе получения кода, заносимого в карту при ее производстве.

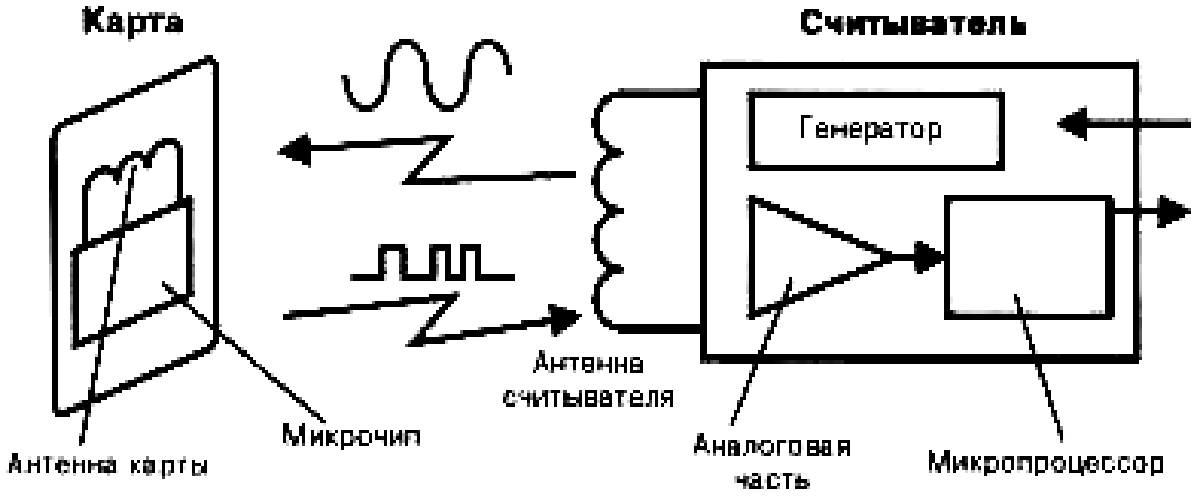


Рисунок 1.83 - Принцип работы Proximity считывателя

Считыватель содержит генератор, работающий, как правило, на частоте 125 кГц, и нагруженный на антенну считывателя. Излучаемая антенной считывателя

энергия принимается антенной карты и запитывает расположенный в карте микрочип. Последний модулирует сигнал в антенне карты кодом, занесенным в микрочип на заводе-изготовителе. Излученный картой сигнал воспринимается антенной считывателя, обрабатывается сначала аналоговой частью схемы считывателя, а затем расположенным в считывателе микропроцессором. Микропроцессор проверяет корректность кода, преобразовывает его к требуемому формату и выдает на выход считывателя, то есть на вход контроллера системы управления доступом.

При всем многообразии форматов данных, обрабатываемых контроллерами систем управления доступом, более 80% систем ориентируются в качестве основного или дополнительного на формат Wiegand 26 бит.

Считыватели «Parsec»

Под торговой маркой «Parsec» производится достаточно широкий спектр оборудования систем управления доступом. В частности, это автономные контроллеры серии ASC-xx и сетевая компьютеризированная система управления доступом ParsecLight. Вместе с тем под этой торговой маркой продается целая гамма Proximity считывателей для применения в существующих системах как отечественного, так и зарубежного производства [71].

Внешний вид считывателей APR-O3xx, APR-04xx и APR-05xx показан на рис. 1.84.

Рисунок 1.84 - Внешний вид считывателей «Parsec»

Особо следует сказать о считывателе APR-05xx, который выполнен в корпусе из нержавеющей стали и предназначен для уличной установки в случаях, когда требуется повышенная защита от вандализма.

1.5.11.5 Технология защиты информации на основе смарт-карт

Появление информационной технологии смарт-карт (СК), основанной на картах со встроенным микропроцессором, позволило удобнее решать вопросы использования пластиковых денег. Однако уникальные возможности СК с микропроцессором, состоящие в высокой степени защиты от подделки, поддержке базовых операций по обработке информации, обеспечении высоких эксплуатационных характеристик, сделали СК одним из лидеров среди носителей конфиденциальной информации [71].

Следует отметить отличительные особенности таких карт. СК содержит микропроцессор и ОС, которые обеспечивают уникальные свойства защиты, имеют контактное и бесконтактное исполнение (на рис. 1.85 показана бесконтактная смарт-карта).

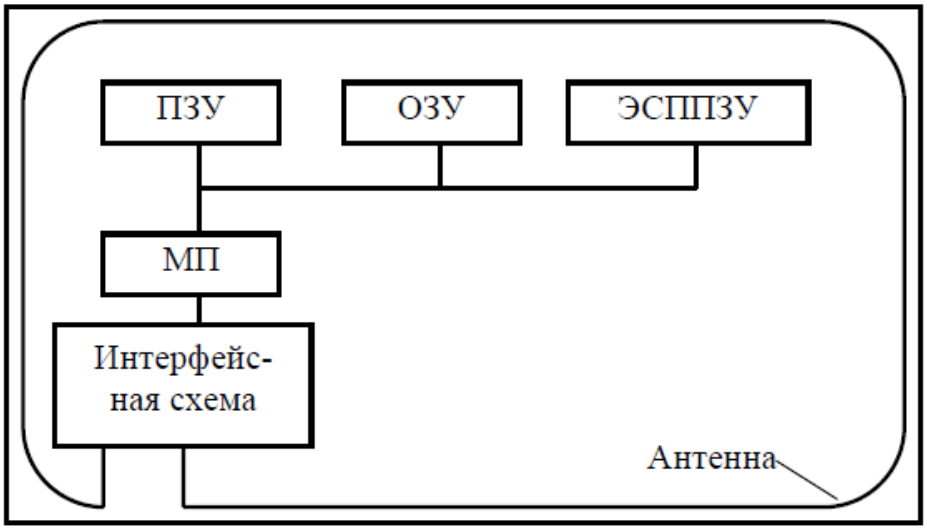


Рисунок 1.85 - Схема бесконтактной смарт-карты

Таким образом, технология СК обеспечивает надежное хранение ключей и доступ к различным информационным ресурсам.

Персональные идентификаторы iKey компании Rainbow являются недорогими брелоками, которые могут использоваться на любой рабочей станции, имеющей универсальную последовательную шину (USB) [71]. Они обеспечивают надежность, простоту и безопасность в такой же степени, как и смарт-карты, но без сложностей и лишних затрат, связанных с использованием считывателя. iKey являются идеальным инструментом для контроля доступа к сетевым службам. iKey 2000 поддерживает и интегрируется со всеми основными прикладными системами, работающими по технологии PKI и используемыми в сетях отдельной организации, нескольких взаимодействующих организаций. Указанные системы включают Microsoft Internet Exolorer и Outlook, Netscape, Entrust, Baltimore, Xcert, Verisign и др. iKey 2000 разрабатывался для защиты цифровой идентичности в рамках инфраструктуры открытых ключей (PKI). iKey 2000 способен с помощью

аппаратных средств генерировать и сохранять в памяти пары открытых ключей и цифровые сертификаты, а также производить цифровую подпись. Личный PKI-ключ недоступен компьютеру клиента.

iKey 2000 создает мощную систему защиты и криптографического кодирования непосредственно внутри аппаратного устройства. Для iKey 2000 пользователю поставляется программное обеспечение. Устройство содержит полный набор криптографических библиотек для браузеров Netscape и Internet Exolorer, а также для клиентов электронной почты. iKey 2000 действует одновременно как смарт-карта и считыватель, находящиеся в едином устройстве с конструктивом USB. Для активизации прикладной программы достаточно вставить iKey 2000 в USB-порт.

iKey 2000 реализует более простой метод обеспечения привилегий пользователя, чем пароли или чисто программные сертификаты. Чтобы запрограммировать ключ, администратору потребуется всего несколько минут. Потерянные ключи могут быть дезактивированы и изменены.

1.5.11.6 Кейс «ТЕНЬ»

Предназначен для транспортировки ноутбуков под охраной с возможностью автоматического уничтожения информации при попытке несанкционированного доступа. Имеет автономный источник питания, дистанционное управление. Монтируется в пыле-, влаго-, взрывозащищенный кейс (рис. 1.86). Также может быть использован для транспортировки жестких дисков, дискет, аудио-, видео-, стримерных кассет [71].

Рисунок 1.86 - Кейс «ТЕНЬ»

Профессиональная модель предназначается для уничтожения в любой момент информации с магнитных носителей при их транспортировке. Имеет повышенную защиту, собственное микропроцессорное управление, автономный источник резервного питания. Изготавливается только под заказ, на основании определенной клиентом комплектации.

Рекомендуется как средство защиты информации (копии, дубликаты, Backup) при ее транспортировке к месту хранения. В базовой комплектации состоит из модуля уничтожения, модуля микропроцессорного управления, модуля резервного питания на 12 ч. Монтируется в стандартный чемодан типа «дипломат». Можно перевозить до 2-х накопителей, под которые рассчитан модуль уничтожения. Активация производится нажатием потайной кнопки, радиобрелка, при попытке несанкционированного вскрытия (защита всего периметра). Питание только от автономного источника питания.

Управление и защита базовых моделей может быть усилена за счет комплектации дополнительными модулями защиты, управления и оповещения.

1.5.11.7 Устройство для быстрого уничтожения информации на жестких магнитных дисках «СТЕК-Н»

Назначение

Изделия «Стек-Н» (рис. 1.87) предназначены для быстрого (экстренного) стирания информации, записанной на накопителях информации, на жестких магнитных дисках, эксплуатируемых, так и не эксплуатируемых в момент стирания [71].

Рисунок 1.87 - Устройство «СТЕК-Н»

Основные особенности изделий серии «Стек»

- предельно возможная скорость уничтожения информации;
- способность находиться во взведенном состоянии сколь угодно долго без ухудшения характеристик;

- возможность применения в дистанционно управляемых системах с автономным электропитанием;

- отсутствие движущихся частей;

- стирание информации, записанной на магнитном носителе, происходит без его физического разрушения, но после стирания использование НЖМД вновь проблематично.

Основные отличительные особенности базовых моделей устройства «Стек-Н»

1) Модель «Стек-НС1» ориентирована на создание рабочего места для быстрого стирания информации с большого количества винчестеров перед их утилизацией. Имеет только сетевое электропитание, характеризуется малым временем перехода в режим «Готовность» после очередного стирания. Модель имеет невысокую стоимость и предельно проста в управлении.

2) Модель «Стек-НС2» ориентирована на создание стационарных информационных сейфов для компьютерных данных, имеет только сетевое электропитание. Модель оборудована системами поддержания температурного режима НЖМД, самотестирования, а также может быть дооборудована модулем дистанционной инициализации.

3) Модель «Стек-НА1» ориентирована на создание портативных информационных сейфов для компьютерных данных, имеет сетевое и автономное электропитание. Модель оборудована системой самотестирования и модулем дистанционной инициализации.

2 ОРГАНИЗАЦИОННО-ПРАВОВАЯ ОСНОВА ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ, ТЕЛЕКОММУНИКАЦИОННЫХ И ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

2.1 Правовое регулирование защиты информации в информационных, телекоммуникационных и информационно-телекоммуникационных системах

25 августа 1991 года, на следующий день после провозглашения Верховной Радой Украины Декларации о независимости, под юрисдикцию Украины были взяты специальные виды связи.

Принятым в марте 1992 года Законом Украины «О Службе безопасности Украины» был законодательно определен порядок обеспечения засекреченной и шифрованной связью государственных органов Украины и соответствующих должностных лиц.

Задачи по развитию и совершенствованию системы специальной связи требовали разработки новых подходов с учетом существующих к тому времени реалий и возможностей. Необходимо было создавать новые системы и средства связи, разрабатывать концепции и современные механизмы обеспечения безопасности и защиты информации в системах специальной связи. Именно тогда, с учетом важности и масштабности поставленных перед подразделением правительственной связи задач, были приняты решения о создании Главного управления правительственной связи (ГУПС СБУ).

Приказом Председателя СБ Украины от 12 октября 1992 года №0160 был утвержден штат ГУПС СБ Украины.

Для формирования отечественной системы криптографической защиты информации с первых дней независимости перед государством стал вопрос сохранения того, что осталось в наследство от СССР - уникального научного потенциала, производственных мощностей, специальных учебных заведений. В феврале 1998 года Указом Президента Украины №110 «О мероприятиях по усовершенствованию криптографической защиты информации в телекоммуникационных и информационных системах» на Главное управление правительственной связи СБ Украины была возложена задача по решению всего комплекса задач, связанных с созданием такой системы в Украине. В мае 1998 года на ГУПС СБ Украины Указом Президента Украины №505 возложено задачу по реализации государственной политики в этой сфере. С целью концентрации усилий в сфере защиты информации по решению Президента Украины в августе 1998 года на базе Главного управления правительственной связи СБ Украины с привлечением специалистов Главного управления технической защиты информации Госкомсекретов был создан Департамент специальных телекоммуникационных систем и защиты информации СБ Украины (ДСТСЗИ СБ Украины), который стал главной структурой в государстве по вопросам криптографической и технической защиты информации.

Широкое внедрение современных информационных технологий, глобализация систем передачи информации поставили перед ДСТСЗИ СБ Украины задачи по защите информационных ресурсов, и в первую очередь информационных ресурсов государственных органов. В связи с этим Указом Президента Украины от 07.11.2005 № 1556/2005 «О соблюдении прав человека во время проведения оперативно-технических мероприятий» определена необходимость создания в государстве **Службы специальной связи и защиты информации Украины**, как центрального органа исполнительной власти со специальным статусом, определив ее основными задачами реализацию государственной политики в сфере защиты государственных информационных ресурсов в сетях передачи данных, обеспечение функционирования Государственной системы правительственной связи, Национальной системы конфиденциальной связи, криптографической и технической защиты информации. Необходимость существования такого государственного органа также определена в Законах Украины «О защите информации в информационно-телекоммуникационных системах», «Об электронной цифровой подписи», «Об электронных документах и электронный документооборот» и т.д.

Вся история развития системы специальной связи, обеспечение безопасности информационного обмена и защиты информации, история создания Государственной службы специальной связи и защиты информации Украины свидетельствуют о понимании важности этих вопросов для становления и прогрессивного развития общества. А результаты деятельности ГУПС - Госспецсвязи являются реальным воплощением правильности избранных подходов по решению этих задач.

Создание на основе ДСТСЗИ СБУ нового государственного органа - Государственной службы специальной связи и защиты информации Украины - является естественным, закономерным шагом эволюционного развития структуры, отвечающей за защиту информации в Украине.

Правовые основы организации и деятельности Государственной службы специальной связи защиты информации Украины определяет Закон Украины « О государственной службе специальной связи и защиты информации Украины» от 23.02.2006 г. Согласно этому Закону, Государственная служба специальной связи и защиты информации Украины является государственным органом, который предназначен для обеспечения функционирования и развития государственной системы правительственной связи, национальной системы конфиденциальной связи, защиты государственных информационных ресурсов в информационных, телекоммуникационных и информационно-телекоммуникационных системах, криптографической и технической защиты информации.

Государственная служба специальной связи и защиты информации Украины подчинена и подконтрольна Президенту Украины.

Общую структуру Государственной службы специальной связи и защиты информации Украины составляют специально уполномоченный центральный орган исполнительной власти по вопросам организации специальной связи и

защите информации и подчиненные ему региональные органы и территориальные подразделения.

Основными задачами Государственной службы специальной связи и защиты информации Украины являются:

- участие в формировании и реализации государственной политики в сфере защиты государственных информационных ресурсов в информационных, телекоммуникационных и информационно-телекоммуникационных системах, криптографической и технической защиты информации;

- обеспечение в установленном порядке правительственной связью Президента Украины, Председателя Верховной Рады Украины, Премьер-министра Украины, других должностных лиц органов государственной власти, органов местного самоуправления, органов военного управления, руководителей предприятий, учреждений и организаций в мирное время, в условиях чрезвычайного и военного положения, а также в случае возникновения чрезвычайной ситуации;

- обеспечение функционирования, безопасности и развития государственной системы правительственной связи и Национальной системы конфиденциальной связи;

- определение требований и порядка создания и развития систем технической и криптографической защиты информации, которая принадлежит к государственным информационным ресурсам, или информации с ограниченным доступом, требование относительно защиты которой установлено законом;

- осуществление государственного контроля за состоянием криптографической и технической защиты информации, которая принадлежит к государственным информационным ресурсам, или информации с ограниченным доступом, требование относительно защиты которой установлено законом, а также за соблюдением требований законодательства в сфере предоставления услуг электронной цифровой подписи;

- охрана объектов, помещений, систем, сетей, комплексов, средств правительственной и специальной связи, ключевых документов и средств криптографической защиты информации Государственной службы специальной связи и защиты информации Украины.

Основными принципами деятельности Государственной службы специальной связи и защиты информации Украины являются:

- законность;

- уважение и соблюдение прав и свобод человека и гражданина;

- единоначалие и централизация управления;

- согласование действий в особый период (в условиях чрезвычайного и военного положения, в случае возникновения чрезвычайной ситуации) с Генеральным штабом Вооруженных Сил Украины, Службой безопасности Украины, центральным органом исполнительной власти по вопросам гражданской защиты;

- открытость для демократического гражданского контроля за соблюдением требований законодательства об охране государственной тайны.

На Государственную службу специальной связи и защиты информации Украины в соответствии с определенными задачами возлагаются следующие обязанности:

1) подготовка предложений по определению общей стратегии и приоритетных направлений деятельности в сфере защиты государственных информационных ресурсов в информационных, телекоммуникационных и информационно-телекоммуникационных системах, криптографической и технической защиты информации;

2) разработка и осуществление мероприятий по развитию систем криптографической и технической защиты информации;

3) разработка порядка и требований по защите государственных информационных ресурсов в информационных, телекоммуникационных и информационно-телекоммуникационных системах, криптографической и технической защиты информации, которая принадлежит к государственным информационным ресурсам, или информации с ограниченным доступом, требование относительно защиты которой установлено законом;

4) обеспечение надежного функционирования, безопасности и развития государственной системы правительственной связи, в частности ее готовности к работе в особый период и в случае возникновения чрезвычайной ситуации;

5) обеспечение в установленном порядке правительственной связью Президента Украины, Председателя Верховной Рады Украины и Премьер-министра Украины в местах их постоянного и временного пребывания;

6) обеспечение в установленном Президентом Украины порядке правительственной связью должностных лиц органов государственной власти, органов местного самоуправления, органов военного управления, руководителей предприятий, учреждений и организаций;

7) участие в выполнении задач территориальной обороны, а также мероприятий, направленных на поддержание правового режима военного и чрезвычайного положения в соответствии с законом;

8) внедрение комплексных систем защиты информации на объектах информационной деятельности и в информационных, телекоммуникационных и информационно-телекоммуникационных системах зарубежных дипломатических учреждений Украины;

9) осуществление мероприятий по организации и обеспечению безопасности и функционирования правительственной связи с зарубежными дипломатическими учреждениями Украины;

10) методическое руководство и координация деятельности органов государственной власти, органов местного самоуправления, военных формирований, предприятий, учреждений и организаций независимо от форм собственности в сфере криптографической и технической защиты информации, а также по вопросам, связанным с предупреждением совершения нарушений безопасности информации в информационных, телекоммуникационных и информационно-телекоммуникационных системах, выявлением и устранением последствий других несанкционированных действий относительно

государственных информационных ресурсов в информационных, телекоммуникационных и информационно-телекоммуникационных системах;

11) накопление и анализ данных о совершении и/или попытке совершения несанкционированных действий относительно государственных информационных ресурсов в информационных, телекоммуникационных и информационно-телекоммуникационных системах, а также об их последствиях, информирование правоохранительных органов для принятия мер по предотвращению и пресечению преступлений в указанной сфере, оценка состояния защищенности государственных информационных ресурсов в информационных, телекоммуникационных и информационно-телекоммуникационных системах, предоставление соответствующих рекомендаций;

12) осуществление мероприятий по созданию, развитию и обеспечению функционирования Национальной системы конфиденциальной связи, обеспечения ее безопасности и оперативно-технического управления;

13) согласование проектов создания информационных, телекоммуникационных и информационно-телекоммуникационных систем, в которых обрабатывается информация, которая принадлежит к государственным информационным ресурсам, или информация с ограниченным доступом, требование относительно защиты которой установлено законом, проведение их экспертной оценки и определение возможности введения в эксплуатацию;

14) согласование и осуществление контроля за выполнением технических заданий на проектирование, строительство и реконструкцию особо важных объектов, разработку образцов военной и специальной техники, в процессе эксплуатации или применения которых собирается, обрабатывается, хранится, передается или принимается информация, которая принадлежит к государственным информационным ресурсам, или информация с ограниченным доступом, требование относительно защиты которой установлено законом;

15) согласование проектов нормативно-правовых актов по вопросам защиты государственных информационных ресурсов в информационных, телекоммуникационных и информационно-телекоммуникационных системах, криптографической и технической защиты информации, которая принадлежит к государственным информационным ресурсам, или информации с ограниченным доступом, требование относительно защиты которой установлено законом, а также по вопросам относительно условий осуществления международных передач криптографических систем, средств криптографической и технической защиты информации, в частности, имеющейся в составе вооружения, военной и специальной техники;

16) установление порядка и требований по использованию информационных, телекоммуникационных и информационно-телекоммуникационных систем, в том числе общего пользования, органами государственной власти, органами местного самоуправления, предприятиями, учреждениями и организациями независимо от форм собственности, которые собирают, обрабатывают, хранят и передают информацию, которая принадлежит к государственным информационным ресурсам, или информации с ограниченным доступом, требование относительно защиты которой установлено законом;

17) выдача и регистрация в соответствии с требованиями законодательства лицензии на осуществление хозяйственной деятельности в сфере криптографической и технической защиты информации, установление порядка выдачи и выдача органам государственной власти разрешения на проведение работ по технической защите информации для собственных потребностей, а также осуществление контроля за соблюдением лицензионных условий и условий проведения работ для собственных нужд;

18) организация и координация совместно с центральным органом исполнительной власти в сфере стандартизации, метрологии и сертификации работ по проведению сертификации средств криптографической и технической защиты информации, организация и проведение государственной экспертизы в сфере криптографической и технической защиты информации;

19) осуществление технического регулирования в сферах защиты государственных информационных ресурсов в информационных, телекоммуникационных и информационно-телекоммуникационных системах, криптографической и технической защиты информации, организация и проведение оценки соответствия, разработка в установленном порядке стандартов, технических регламентов, технических условий;

20) разработка и сопровождение моделей технических разведок путем сбора и анализа информации о существующих системах и средствах технических разведок, тактику и методы их применения, а также перспективы развития, предоставление рекомендаций органам государственной власти, органам местного самоуправления, воинским формированиям, предприятиям, учреждениям и организациям по обеспечению противодействия техническим разведкам, проведение оценки угроз и принятия мер необходимых для защиты информации;

21) участие в пределах своих полномочий в согласовании вопросов размещения на территории Украины дипломатических представительств и консульских учреждений иностранных государств;

22) разработка и организация выполнения научных и научно-технических программ по направлениям ее деятельности;

23) осуществление государственного контроля за состоянием криптографической и технической защиты информации, которая принадлежит к государственным информационным ресурсам, или информации с ограниченным доступом, требование относительно защиты которой установлено законом, в органах государственной власти, органах местного самоуправления, воинских формированиях, на предприятиях, в учреждениях и организациях независимо от форм собственности, в том числе в зарубежных дипломатических учреждениях Украины, местах постоянного и временного пребывания Президента Украины, Председателя Верховной Рады Украины и Премьер-министра Украины, а также во время деятельности на территории Украины иностранных инспекционных групп в соответствии с международными договорами Украины, согласие на обязательность которых дано Верховной Радой Украины;

24) осуществление государственного контроля за соблюдением требований безопасности в процессе разработки, производства, использования, эксплуатации,

сертификационных испытаний, тематических исследований, экспертизы, ввоза, вывоза и уничтожения криптографических систем и средств криптографической защиты информации и оборудования специальной связи;

25) представление Президенту Украины по результатам государственного контроля аналитических материалов о состоянии криптографической и технической защиты информации в государстве, разработка рекомендаций по его улучшению;

26) осуществление государственного контроля за соблюдением требований законодательства в сфере предоставления услуг электронной цифровой подписи;

27) осуществление приема и контроля качества продукции, других товаров военного назначения, которые производятся или модернизируются по ее заказу;

28) разработка, изготовление и поставка ключевых документов к средствам криптографической защиты информации содержащей государственную тайну, и конфиденциальной информации, которая принадлежит к государственным информационным ресурсам;

29) организация и осуществление совместно с центральным органом исполнительной власти в области образования научно-методического управления подготовкой кадров в сфере криптографической и технической защиты информации;

31) согласование международных передач криптографических систем, средств криптографической и технической защиты информации, в частности в составе вооружения, военной и специальной техники;

32) выдача аттестата соответствия комплексных систем защиты информации информационных, телекоммуникационных и информационно-телекоммуникационных систем, с применением которых обрабатывается информация, которая принадлежит к государственным информационным ресурсам, или информация с ограниченным доступом, требование относительно защиты которой установлено законом, требованиями нормативных документов по вопросам технической защиты информации;

33) осуществление в порядке, определенном Кабинетом Министров Украины, государственного контроля за соблюдением условий эксплуатации комплексных систем защиты информации, прошедших государственную экспертизу и на которые выдан аттестат соответствия;

34) установление порядка осуществления государственного контроля за соблюдением требований законодательства в сфере предоставления услуг электронной цифровой подписи, а также состоянием криптографической и технической защиты информации, которая принадлежит к государственным информационным ресурсам, или информации с ограниченным доступом, требование относительно защиты которой установлено законом, а также при осуществлении деятельности на территории Украины иностранных инспекционных групп в соответствии с международными договорами Украины.

Должностные лица соответствующих подразделений Государственной службы специальной связи и защиты информации Украины несут ответственность согласно закону за нарушение конституционных прав и свобод человека и гражданина в процессе использования средств специальной связи.

Для обеспечения выполнения возложенных на нее задач Государственная служба специальной связи и защиты информации Украины имеет право:

1) получать в установленном порядке по письменным запросам руководителей соответствующих органов и территориальных подразделений Государственной службы специальной связи и защиты информации Украины от органов государственной власти, органов местного самоуправления, воинских формирований, предприятий, учреждений и организаций независимо от форм собственности информацию, документы и материалы, необходимые для выполнения возложенных на нее задач;

2) привлекать специалистов органов государственной власти, органов местного самоуправления, воинских формирований, предприятий, учреждений и организаций независимо от форм собственности по согласованию с их руководителями для рассмотрения вопросов, относящихся к ее полномочий, а также проведение совместных инспекционных проверок;

3) доступа в установленном порядке своих уполномоченных представителей на объекты органов государственной власти, органов местного самоуправления, воинских формирований, предприятий, учреждений и организаций независимо от форм собственности, на которых находятся средства специальной связи, а также объекты, по которым осуществляется государственный контроль за состоянием криптографической и технической защиты информации, которая принадлежит к государственным информационным ресурсам, или информации с ограниченным доступом, требование относительно защиты которой установлено законом;

4) предоставлять на договорных началах помощь предприятиям, учреждениям и организациям независимо от форм собственности в разработке и осуществлении мер по защите информационных ресурсов в информационных, телекоммуникационных и информационно-телекоммуникационных системах, криптографической и технической защиты информации;

5) осуществлять плановые и внеплановые инспекционные проверки состояния криптографической и технической защиты информации, которая принадлежит к государственным информационным ресурсам, или информации с ограниченным доступом, требование относительно защиты которой установлено законом, в органах государственной власти, органах местного самоуправления, воинских формированиях, на предприятиях, в учреждениях и организациях независимо от форм собственности, в том числе в зарубежных дипломатических учреждениях Украины, без получения доступа к содержанию информации;

6) приостанавливать действие или отменять в установленном порядке лицензии на осуществление хозяйственной деятельности в сфере криптографической и технической защиты информации, а также разрешений на проведение работ по технической защите информации для собственных нужд органами государственной власти;

7) ставить в установленном порядке вопрос о прекращении информационной деятельности с использованием информационных, телекоммуникационных и информационно-телекоммуникационных систем в органах государственной власти, органах местного самоуправления, воинских формированиях, на предприятиях, в учреждениях и организациях независимо от

форм собственности в случае нарушения ими требований законодательства в сфере защиты государственных информационных ресурсов, криптографической и/или технической защиты информации;

8) получать в установленном порядке полосы радиочастот для использования радиосредствами специальной связи;

9) привлекать специальных и общих пользователей радиочастотного ресурса для выявления и устранения радиопомех радиоэлектронным средствам государственной системы правительственной связи и Национальной системы конфиденциальной связи;

10) организовывать, проводить и выполнять научно-исследовательские, опытно-конструкторские работы;

11) выступать государственным заказчиком по оборонному заказу и заказчиком закупки товаров, работ и услуг за государственные средства;

12) выступать заказчиком строительства объектов Государственной службы специальной связи и защиты информации Украины;

13) образовывать координационные, консультативные и совещательные органы;

14) осуществлять в установленном порядке издательскую деятельность;

15) осуществлять в порядке, предусмотренном законодательством, хозяйственную деятельность, которая непосредственно связана с обеспечением выполнения возложенных на нее задач, по видам деятельности, перечень которых определяется Кабинетом Министров Украины;

16) отчуждать в порядке, предусмотренном законодательством, закрепленное за ней государственное имущество;

17) составлять протоколы об административных правонарушениях;

18) осуществлять международное сотрудничество по вопросам, относящимся к ее компетенции, разрабатывать предложения по заключению соответствующих международных договоров Украины, взаимодействовать в соответствии с международными договорами Украины с международными организациями по вопросам предотвращения нарушения безопасности информации в информационных, телекоммуникационных и информационно-телекоммуникационных системах.

19) проводить плановую и внеплановую проверку соблюдения лицензионных условий осуществления хозяйственной деятельности в сфере криптографической и технической защиты информации на предприятиях, в учреждениях и организациях, а также условий проведения работ по технической защите информации для собственных нужд в органах государственной власти;

20) приостанавливать действие или отменять в установленном порядке аттестаты соответствия на комплексные системы защиты информации в информационных, телекоммуникационных и информационно-телекоммуникационных системах;

21) проводить плановую и внеплановую проверку центрального удостоверяющего органа, удостоверяющих центров и центров сертификации ключей относительно соблюдения ими требований законодательства в сфере предоставления услуг электронной цифровой подписи;

22) обращаться в суд в случае возникновения споров по вопросам организации специальной связи и защиты информации, криптографической и технической защиты информации, которая принадлежит к государственным информационным ресурсам, или информации с ограниченным доступом, требование относительно защиты которой установлено законом, споров в сфере предоставления услуг электронной цифровой подписи, а также в случае возникновения других споров в порядке, установленном законом.

Специально уполномоченный центральный орган исполнительной власти по вопросам организации специальной связи и защиты информации в пределах своих полномочий на основе и в соответствии с законодательством издает приказы, организовывает и контролирует их выполнение.

Приказы специально уполномоченного центрального органа исполнительной власти по вопросам организации специальной связи и защиты информации, принятые в пределах его полномочий, обязательны для исполнения органами государственной власти, органами местного самоуправления, военными формированиями, предприятиями, учреждениями и организациями независимо от форм собственности и физическими лицами.

Информация, которая циркулирует в информационно-телекоммуникационных системах, довольно часто является информацией с ограниченным доступом. На сегодня отношения в сфере защиты информации в информационных, телекоммуникационных и информационно-телекоммуникационных системах (далее - системах) регулируются Законом Украины «О защите информации в информационно-телекоммуникационных системах» от 05.07.94 г. Закон устанавливает основы регулирования правовых отношений относительно защиты информации в системах при условии соблюдения права собственности граждан Украины и юридических лиц на информацию и права доступа к ней, с одной стороны, права владельца информации на ее защиту, а также установленного действующим законодательством ограничения на доступ к информации, с другой.

Так, Законом определены объекты защиты в системе – это информация, которая обрабатывается в ней, и программное обеспечение, которое предназначено для обработки этой информации.

Субъектами отношений, связанных с защитой информации в системах, являются:

- владельцы информации;
- владельцы системы;
- пользователи;
- специально уполномоченный центральный орган исполнительной власти по вопросам организации специальной связи и защиты информации и подчиненные ему региональные органы.

На основании заключенного договора или по поручению владелец информации может предоставить право распоряжаться информацией другому физическому или юридическому лицу - распорядителю системы.

Порядок доступа к информации, перечень пользователей и их полномочия относительно этой информации определяются собственником информации.

Порядок доступа к информации, которая принадлежит к государственным информационным ресурсам, или информации с ограниченным доступом, требование относительно защиты которой установлено законом, перечень пользователей и их полномочия относительно этой информации определяются законодательством.

В случаях, предусмотренных законом, доступ к информации в системе может осуществляться без разрешения его собственника в порядке, установленном законом.

Владелец системы обеспечивает защиту информации в системе в порядке и на условиях, определенных в договоре, который заключается ним с владельцем информации, если иное не предусмотрено законом.

Владелец системы по требованию владельца информации предоставляет сведения по защите информации в системе.

Владелец системы предоставляет пользователю сведения о правилах и режиме работы системы и обеспечивает ему доступ к информации в системе в соответствии с определенным порядком доступа.

Владелец системы, которая используется для обработки информации с другой системы, обеспечивает защиту такой информации в порядке и на условиях, определяемых договором, который заключается между владельцами систем, если иное не установлено законодательством.

Владелец системы, которая используется для обработки информации с другой системы, сообщает владельцу указанной системы о выявленных фактах несанкционированных действий относительно информации в системе.

Условия обработки информации в системе определяются собственником системы согласно договору с владельцем информации, если иное не предусмотрено законодательством.

Информация, которая принадлежит к государственным информационным ресурсам, или информация с ограниченным доступом, требование относительно защиты которой установлено законом, должна обрабатываться в системе с применением комплексной системы защиты информации с подтвержденным соответствием. Подтверждение соответствия осуществляется по результатам государственной экспертизы в порядке, установленном законодательством.

Для создания комплексной системы защиты информации, которая принадлежит к государственным информационным ресурсам, или информации с ограниченным доступом, требование по защите которой установлено законом, используются средства защиты информации, имеющие сертификат соответствия или положительное экспертное заключение по результатам государственной экспертизы в сфере технической и/или криптографической защиты информации. Подтверждение соответствия и проведение государственной экспертизы этих средств осуществляются в порядке, установленном законодательством.

Ответственность за обеспечение защиты информации в системе возлагается на владельца системы.

Владелец системы, в которой обрабатывается информация, которая принадлежит к государственным информационным ресурсам, или информация с ограниченным доступом, требование по защите которой установлено законом,

формирует службу защиты информации или назначает лиц, на которых возлагается обеспечение защиты информации и контроль за ней.

О попытках и/или фактах несанкционированных действий в системе по информации, которая принадлежит к государственным информационным ресурсам, или информации с ограниченным доступом, требование относительно защиты которой установлено законом, владелец системы сообщает соответственно в специально уполномоченный центральный орган исполнительной власти по вопросам организации специальной связи и защиты информации или подчиненный ему региональный орган.

Требования по обеспечению защиты информации, которая принадлежит к государственным информационным ресурсам, или информации с ограниченным доступом, требование по защите которой установлено законом, устанавливаются Кабинетом Министров Украины.

Специально уполномоченный центральный орган исполнительной власти по вопросам организации специальной связи и защиты информации:

- разрабатывает предложения относительно государственной политики в сфере защиты информации и обеспечивает ее реализацию в пределах своей компетенции;

- определяет требования и порядок создания комплексной системы защиты информации, которая принадлежит к государственным информационным ресурсам, или информации с ограниченным доступом, требование относительно защиты которой установлено законом;

- организует проведение государственной экспертизы комплексных систем защиты информации, экспертизы и подтверждения соответствия средств технической и криптографической защиты информации;

- осуществляет контроль за обеспечением защиты информации, которая принадлежит к государственным информационным ресурсам, или информации с ограниченным доступом, требование по защите которой установлено законом;

- осуществляет мероприятия по выявлению угрозы государственным информационным ресурсам от несанкционированных действий в информационных, телекоммуникационных и информационно-телекоммуникационных системах и дает рекомендации по вопросам предотвращения такой угрозы.

Государственные органы в пределах своих полномочий по согласованию соответственно со специально уполномоченным центральным органом исполнительной власти по вопросам организации специальной связи и защиты информации или подчиненным ему региональным органом устанавливают особенности защиты информации, которая принадлежит к государственным информационным ресурсам, или информации с ограниченным доступом, требование относительно защиты которой установлено законом.

Особенности защиты информации в системах, обеспечивающих банковскую деятельность, устанавливаются Национальным банком Украины.

Отношения, которые возникают по поводу защиты информации в информационно-телекоммуникационных системах, также частично регулируются Законом Украины «Об электронных документах и электронном

документообороте» от 22.05.2003 г. Предметом правового регулирования данного Закона являются отношения, которые возникают в процессе создания, отправления, передачи, получения, хранения, обработки, использования и уничтожения электронных документов.

Порядок осуществления криптографической защиты информации в Украине определяется «Положением о порядке осуществления криптографической защиты информации в Украине», утвержденным Указом Президента Украины от 22.05.1998 г. №505, а также «Инструкцией о порядке поставки и использования ключей для средств криптографической защиты информации», утвержденной Администрацией Государственной службы специальной связи и защиты информации в Украине от 12.06.2007 г. №114.

В частности, Положение определяет порядок осуществления криптографической защиты информации с ограниченным доступом, разглашение которой приносит вред государству, обществу или личности.

Концепция технической защиты информации в Украине утверждена Постановлением Кабинета Министров Украины от 08.10.1997 г. №1126.

Концепция определяет основы государственной политики в области защиты информации инженерно-техническими средствами. Техническая защита информации является составной частью обеспечения национальной безопасности Украины и направлена на обеспечение инженерно-техническими средствами порядка доступа, целостности и доступности (невозможности блокирования) информации с ограниченным доступом, а также целостности и доступности открытой информации, важной для личности, общества и государства.

Указом Президента Украины от 27.09.1999 г. №1229 утверждено «Положение о технической защите информации в Украине». Это Положение определяет правовые и организационные основы технической защиты информации важной для государства, общества и личности, охрана которой обеспечивается государством в соответствии с законодательством.

В частности, правовую основу технической защиты информации в Украине составляют Конституция Украины, законы Украины, акты Президента Украины и Кабинета Министров Украины, нормативно-правовые акты Службы безопасности Украины, Администрация Государственной службы специальной связи и защите информации Украины, других государственных органов, международные договора Украины, согласие на обязательное выполнение которых дано Верховной Радой Украины, по вопросам технической защиты информации.

Государственная политика технической защиты информации формируется согласно с законодательством и реализуется Государственной службой специальной связи и защиты информации Украины (Госспецсвязь Украины) во взаимодействии с органами, в отношении которых осуществляется техническая защита информации (ТЗН). Такими органами являются: органы государственной власти; органы местного самоуправления; органы управления Вооруженных Сил Украины и других военных формирований, созданных согласно законодательству Украины; соответствующие предприятия, учреждения, организации.

Организация технической защиты информации в органах, в отношении которых осуществляется ТЗИ, возлагается на их руководителей.

Организационно-технические принципы, порядок осуществления мероприятий по технической защите информации, порядок контроля в этой сфере, характеристики угроз для информации, нормы и требования по технической защите информации, порядок аттестации и экспертизы комплексов технической защиты информации определяются нормативно-правовыми актами, принятыми в установленном порядке соответствующими органами.

Нормативно-правовые акты по технической защите информации является обязательными для выполнения всеми субъектами системы технического защиты информации.

Разработка, издание нормативно-правовых актов по вопросам технической защиты информации, а также работы, связанные с разработкой и выполнением общегосударственных программ развития системы технической защиты информации, осуществляются за счет средств государственного бюджета и других источников финансирования, не запрещенных законодательством.

Субъектами системы технической защиты информации являются:

- Госспецсвязь Украины;
- органы, в отношении которых осуществляется ТЗИ;
- научно-исследовательские и научно-производственные учреждения Госспецсвязи Украины, государственные предприятия, находящиеся в управлении Госспецсвязи Украины и выполняющие задачи по технической защите информации;
- воинские части, предприятия, учреждения и организации всех форм собственности и граждане-предприниматели, осуществляющие деятельность по технической защите информации по соответствующим документам или лицензиями;
- учебные заведения по подготовке, переподготовке и повышению квалификации специалистов по технической защите информации.

Основными задачами органов, в отношении которых осуществляется ТЗИ, являются:

- обеспечение технической защиты информации в соответствии с требованиями нормативно-правовых актов по вопросам технической защиты информации;
- издание в пределах своих полномочий нормативно-правовых актов по указанным вопросам;
- осуществление контроля за состоянием технической защиты информации.

Органы, относительно которых осуществляется ТЗИ, согласно возложенных на них задач:

- создают или определяют подразделения, на которые возлагается обеспечения технической защиты информации и контроль за его состоянию, согласовывают основные задачи и функции этих подразделений;
- выдают по согласованию с Администрацией Госспецсвязи Украина и внедряют нормативно-правовые акты по вопросам технической защиты информации;
- согласовывают с Администрацией Госспецсвязи Украины проведение предприятиями, учреждениями, организациями тех научно-исследовательских,

опытно-конструкторских и опытно-технологических работ, направленных на развитие нормативно-правовой и материально-технической базы системы технической защиты информации, которые осуществляются за счет средств государственного бюджета;

- создают или определяют по согласованию с Администрацией Госспецсвязи Украины предприятия, учреждения и организации, обеспечивают техническую защиту информации;

- обеспечивают подготовку, переподготовку и повышение квалификации кадров по технической защите информации;

- предоставляют Администрации Госспецсвязи Украины по ее запросам сведения о состоянии технической защиты информации.

Основными задачами других субъектов системы технической защиты информации являются:

- исследование угроз для информации на объектах, функционирование которых связано с информацией, подлежащей охране;

- создание и производство средств обеспечения технической защиты информации;

- разработка, внедрение, сопровождение комплексов технической защиты информации;

- повышение квалификации специалистов по технической защите информации.

При разработке и внедрении мероприятий по технической защите информации используются средства, разрешенные Администрацией Госспецсвязи Украины, для применения и включенные в соответствующие перечни.

Контроль в сфере технической защиты информации заключается в проверке выполнения требований Положения о технической защите информации в Украине, других нормативно-правовых актов по вопросам технической защиты информации и в оценке защищенности информации на объекте, где она циркулировала или циркулирует.

Оценка защищенности информации осуществляется путем аттестации или экспертизы комплексов технической защиты информации и инспекционных проверок. По результатам аттестации или экспертизы комплексов технической защиты информации определяется возможность введения в эксплуатацию объекта, где циркулирует информация, охрана которой обеспечивается государством.

Порядок экспертизы и инспекционных проверок защищенности информации определяется соответствующими нормативно-правовыми актами.

Разработка, внедрение, аттестация и эксплуатация комплексов технической защиты информации для собственных нужд осуществляются соответствующими подразделениями органов, в отношении которых осуществляется ТЗИ, или воинскими частями, предприятиями, учреждениями, организациями, на которые в установленном порядке возложено обеспечение технической защиты информации, при наличии у них соответствующего разрешения.

К выполнению этих работ могут быть привлечены субъекты предпринимательской деятельности, имеющие соответствующие лицензии.

Результаты аттестации на государственных объектах, отнесенных заказчиком к особо важным, согласовываются с Администрацией Госспецсвязи Украины.

Работы по технической защите информации в органах, по которым осуществляется ТЗИ, осуществляются за счет средств, выделяемых на их содержание, прибыли и других источников, не запрещенных законодательством.

Руководители указанных органов создают надлежащие условия для контроля за обеспечением технической защиты информации.

В случае нарушения требований по обеспечению технической защиты информации должностные лица и граждане несут ответственность согласно законодательству Украины.

Постановлением Кабинета Министров Украины от 29.03.2006 г. №373 утверждены «Правила обеспечения защиты информации в информационных, телекоммуникационных и информационно-телекоммуникационных системах». Эти правила определяют общие требования и организационные основы обеспечения защиты информации, которая принадлежит к государственным информационным ресурсам, или информации с ограниченным доступом, требование по защите которой определено законом, в информационных, телекоммуникационных и информационно-телекоммуникационных системах.

Защите в системе подлежит:

- открытая информация, которая относится к государственным информационным ресурсам и по определению Закона Украины «Об информации», относится к статистической, правовой, социологической информации, информация справочно-энциклопедического характера и используется для обеспечения деятельности государственных органов местного самоуправления, а также информация о деятельности указанных органов, которая распространяется в Интернете, других глобальных информационных сетях и системах или передается телекоммуникационными сетями;

-служебная информация, которая относится к государственным информационным ресурсам;

- конфиденциальная информация о физическом лице, а также информация, доступ к которой ограничен физическим или юридическим лицом;

- секретная информация.

Требования по обеспечению защиты информации в системе

Открытая информация во время обработки в системе должна сохранять целостность, которая обеспечивается путем защиты от несанкционированных действий, которые могут привести к ее случайной или умышленной модификации или уничтожению.

Всем пользователям должен быть обеспечен доступ к ознакомлению с открытой информацией. Модифицировать или уничтожать открытую информацию могут только идентифицированные и аутентифицированные пользователи, которым предоставлены соответствующие полномочия.

Попытки модификации или уничтожения открытой информации пользователями, которые не имеют на это полномочий, неидентифицированными

пользователями или пользователями неподтвержденными при аутентификации соответствием предъявленного идентификатора, должны блокироваться.

При обработке служебной и секретной информации должна обеспечиваться ее защита от несанкционированного и неконтролируемого ознакомления, модификации, уничтожения, копирования, распространения.

Доступ к служебной информации предоставляется только идентифицированным и аутентифицированным пользователям. Попытки доступа к такой информации неидентифицированных лиц или пользователей с неподтвержденным при аутентификации соответствием предъявленного идентификатора, должны блокироваться.

В системе обеспечивается возможность предоставления пользователю права на выполнение одной или нескольких операций по обработке конфиденциальной или служебной информации или лишения его такого права.

Требования к защите в системе информации, составляющей государственную тайну, определяются Правилами обеспечения защиты информации в телекоммуникационных и информационно-телекоммуникационных системах и законодательством в сфере охраны государственной тайны.

Обеспечение защиты в системе секретной информации, не составляющей государственную тайну, осуществляется согласно требованиям к защите служебной информации, если иное не предусмотрено законом.

Требования к защите в системе информации от несанкционированного блокирования определяются распорядителем информации, если иное для этой информации или системы, в которой она обрабатывается, не установлено законодательством.

В системе осуществляется обязательная регистрация:

- результатов идентификации и аутентификации пользователей;
- результатов выполнения пользователем операций по обработке информации;
- попыток несанкционированных действий с информацией;
- фактов предоставления и лишения пользователей права доступа к информации и ее обработке;
- результатов проверки целостности средств защиты информации.

Обеспечивается возможность проведения анализа регистрационных данных исключительно пользователем, который уполномочен осуществлять управление средствами защиты информации и контроль за защитой информации в системе (администратор безопасности).

Регистрация осуществляется автоматическим способом, а регистрационные данные защищаются от модификации и уничтожения пользователями, которые не имеют полномочий администратора безопасности.

Регистрация попыток несанкционированных действий с информацией, составляющей государственную тайну, а также конфиденциальной информации о физическом лице, законом отнесенной к персональным данным, должна сопровождаться уведомлением о них администратора безопасности.

Идентификация и аутентификация пользователей, предоставление и лишение их права доступа к информации и ее обработке, контроль за целостностью средств защиты в системе осуществляется автоматизированным способом.

Передача информации с ограниченным доступом из одной системы к другой осуществляется в зашифрованном виде или защищенными каналами связи в соответствии с требованиями законодательства по вопросам технической и криптографической защиты информации.

Порядок подключения систем, в которых обрабатывается информация с ограниченным доступом, к глобальным сетям передачи данных определяется законодательством.

В системе осуществляется контроль за целостностью программного обеспечения, которое используется для обработки информации, предотвращением несанкционированной его модификации и ликвидации последствий такой модификации.

Контролируется также целостность программных и технических средств защиты информации. В случае нарушения их целостности обработка в системе информации прекращается.

Организационные основы обеспечения защиты информации

Для обеспечения защиты информации в системе создается комплексная система защиты информации, которая предназначается для защиты информации от:

- утечки по техническим каналам, к которым относятся каналы побочных электромагнитных излучений и наводок, акустические, электрические и другие каналы, которые образуются под воздействием физических процессов при функционировании средств обработки информации, других технических средств и коммуникаций;

- несанкционированных действий с информацией, в том числе с использованием компьютерных вирусов;

- специального воздействия на средства обработки информации, осуществляемого путем формирования физических полей и сигналов, которое может привести к нарушению ее целостности и несанкционированной блокировки.

Защита информации от утечки по техническим каналам обеспечивается в системе в случае, когда в ней обрабатывается информация, составляющая государственную тайну, или когда соответствующее решение о необходимости такой защиты принято распорядителем информации.

Защита информации от несанкционированных действий, в том числе от компьютерных вирусов, обеспечивается во всех системах.

Защита информации от специального влияния на средства обработки информации обеспечивается в системе, если решение о необходимости такой защиты принято распорядителем информации.

Ответственность за обеспечение защиты информации в системе, своевременная разработка необходимых для этого мероприятий и создание системы защиты возлагается на руководителя (заместителя руководителя)

организации, являющейся владельцем (распорядителем) системы, и руководителей ее структурных подразделений, обеспечивающих создание и эксплуатацию системы.

Организация и проведение работ по защите информации в системе осуществляется службой защиты информации, которая обеспечивает определенные требования к защите информации в системе, проектированию, разработке и модернизации системы защиты, а также выполнению работ по ее эксплуатации и контролю за состоянием защищенности информации.

Служба защиты информации создается согласно решению руководителя организации, являющегося владельцем (распорядителем) системы.

В случае если объем работ, связанных с защитой информации в системе, является незначительным, защита информации может осуществляться одним лицом.

Защита информации на всех этапах создания и эксплуатации системы осуществляется в соответствии с разработанным службой защиты информации планом защиты информации в системе.

План защиты информации в системе содержит:

- задачи защиты, классификацию информации, которая обрабатывается в системе, описание технологии обработки информации;

- определения модели угроз для информации в системе;

- основные требования по защите информации и правила доступа к ней в системе;

- перечень документов, согласно которым осуществляется защита информации в системе;

- перечень и сроки выполнения работ службой защиты информации.

Требования и порядок создания системы защиты устанавливаются Администрацией Госспецсвязи (далее - Администрация).

Требования к защите информации каждой отдельной системы устанавливаются техническим заданием на создание системы или системы защиты.

В составе системы защиты должны использоваться средства защиты информации с подтвержденным соответствием.

В случае использования средств защиты информации, которые не имеют подтверждения соответствия на момент проектирования системы защиты, соответствующее оценивание проводится при государственной экспертизе системы защиты.

Порядок проведения государственной экспертизы системы защиты, государственной экспертизы и сертификации средств технической и криптографической защиты информации устанавливается Администрацией.

Органы исполнительной власти, которые имеют разрешение на осуществление деятельности по технической защите информации для собственных нужд, вправе с согласия департамента организовывать проведение государственной экспертизы системы защиты на предприятиях, в учреждениях и организациях, которые принадлежат к сфере их управления. Порядок проведения

такой экспертизы устанавливается органом исполнительной власти по согласованию с Администрацией.

Исполнителем работ по созданию системы защиты может быть субъект хозяйственной деятельности или орган исполнительной власти, имеющий лицензию или разрешение на право осуществления хотя бы одного вида работ в области технической защиты информации, необходимость проведения которого определено техническим заданием на создание системы защиты.

Для проведения других видов работ по технической защите информации, на проведение которых исполнитель не имеет лицензии (разрешения), привлекаются соисполнители, имеющие соответствующие лицензии.

Если для создания системы защиты необходимо провести работы по криптографической защите информации, исполнитель должен иметь лицензии на осуществление вида работ в области криптографической защиты информации или привлекать соисполнителей, имеющих соответствующие лицензии.

Контроль за обеспечением защиты информации в системе заключается в проверке выполнения требований по технической и криптографической защите информации и осуществляется в порядке, определенном Администрацией.

В системе, состоящей из нескольких информационных и/или телекоммуникационных систем, эти правила могут применяться к каждой составной части отдельно.

Разработка, создание и эксплуатация конкретных информационных, телекоммуникационных и информационно-телекоммуникационных систем с целью защиты информации должна осуществляться с учетом положений таких нормативных документов:

- НД ТЗИ 11-002-99 Общие положения относительно защиты информации в компьютерных системах от несанкционированного доступа;

- НД ТЗИ 2.5-005-99 Классификация автоматизированных систем и стандартные функциональные профили защищенности обрабатываемой информации от несанкционированного доступа;

- НД ТЗИ 2.5-004-99 Критерии оценки защищенности информации в компьютерных системах от несанкционированного доступа;

НД ТЗИ 14-001-2000 Типовое положение о службе защиты информации в автоматизированной системе;

- НД ТЗИ 3.7-0001-99 Методические указания по разработке технического задания на создание комплексной системы защиты информации в автоматизированной системе;

- НД ТЗИ 3.6-001-2000 Техническая защита информации. Компьютерные системы. Порядок создания, внедрения, сопровождения и модернизации средств технической защиты информации от несанкционированного доступа;

- НД ТЗИ 2.5-008-2002 Требования по защите конфиденциальной информации от несанкционированного доступа при обработке в автоматизированных системах класса 2;

- НД ТЗИ 3.7-003-05 Порядок проведения работ по созданию комплексной системы защиты информации в информационно-телекоммуникационной системе;

- НД ТЗИ 2.5-010-03 Требования к защите информации WEB-страницы от несанкционированного доступа;

- Временные рекомендации по технической защите от утечки каналами побочных электромагнитных излучений и наводок (ВР ТЗИ-ПЭМИ-95);

- Временные рекомендации по технической защите информации в средствах вычислительной техники, автоматизированных системах и сетях от утечки каналами побочных электромагнитных излучений и наводок (ВР ЭВТ-95);

- Временное положение о категорировании объектов (ВПКО-95).

Эти нормативные документы были утверждены приказами Департамента специальных телекоммуникационных систем и защиты информации Службы безопасности Украины. Наряду с этим, приказами Администрации Государственной службы специальной связи и защиты информации Украины утвержден ряд положений, направленных на усиление государственного контроля по технической защите информационных ресурсов и сертификации средств защиты информации.

Так, приказом Государственной службы специальной связи и защиты информации Украины от 25.04.07 г. №75/91 утверждены «Правила проведения работ по сертификации средств защиты информации», приказом от 16.05.07 г. №87 – «Положение о государственном контроле за состоянием технической защиты информации»; приказом от 16.05.07 г. №93 – «Положение о государственной экспертизе в сфере технической защиты информации»; приказом от 04.07.08 г. №112 утвержден «Порядок оценки состояния защищенности государственных информационных ресурсов в информационных, телекоммуникационных и информационно-телекоммуникационных системах».

Рассмотрим некоторые положения нормативных документов.

Нормативный документ технической защиты информации «Общие положения относительно защиты информации в компьютерных системах от несанкционированного доступа (НД ТЗИ 11-002-99) определяет методологические основы (концепцию) решения задач защиты информации в компьютерных системах и создания нормативных и методологических документов, регламентирующих вопросы:

- определения требований по защите компьютерных систем от несанкционированного доступа;

- создания защищенных компьютерных систем и средств их защиты от несанкционированного доступа;

- оценки защищенности компьютерных систем и их способности решения задач потребителя.

Защита информации, которая обрабатывается в информационных, телекоммуникационных, информационно-телекоммуникационных системах заключается в создании и поддержании в рабочем состоянии систему мер как технических (инженерных, программно-аппаратных) так и организационных, правовых, что позволяет избежать или усложнить возможность реализации угроз, а также снизить потенциальный ущерб. Система мер, которая обеспечивает защиту информации в информационных, телекоммуникационных,

информационно-телекоммуникационных системах, называется комплексной системой защиты информации (КСЗИ).

Часть проблем обеспечения защиты информации в системах могут быть решены организационными мерами. Однако с развитием информационных технологий наблюдается тенденция роста необходимости использования технических мер и средств защиты.

Информационные, телекоммуникационные и информационно-телекоммуникационные системы представляют собой организационно-технические системы, которые объединяют вычислительную систему, физическую среду, персонал и обрабатываемую информацию.

Принято различать два основных направления технической защиты информации в системах – защита системы и обрабатываемой информации от несанкционированного доступа и защита информации от утечки по техническим каналам.

Угрозы обрабатываемой в системе информации зависят от характеристик самой системы, физической среды, персонала и обрабатываемой информации. Угрозы могут иметь или объективную природу (смена условий физической среды, отказ элементов системы), или субъективную (ошибка персонала, действие преступника). Угрозы, имеющие субъективную природу, могут быть случайными или целенаправленными. Попытка реализации угрозы называется атакой.

Из всех способов классификации угроз наилучшей для анализа является классификация угроз по результатам их влияния на информацию, то есть нарушения конфиденциальности, целостности и доступности информации.

Информация сохраняет конфиденциальность, если соблюдаются установленные правила ознакомления с ней. Информация сохраняет целостность, если соблюдаются установленные правила ее модификации (удаление, изменение). Информация сохраняет доступность, если сохраняется возможность ознакомления с ней или ее модификации в соответствии с установленными правилами в течение какого-либо определенного промежутка времени. Угрозы, реализация которых приводит к утере информации какой либо из названных свойств, соответственно являются угрозами конфиденциальности, целостности или доступности информации.

Компьютерные системы, как правило, состоят из множества компонентов. Некоторые из них могут быть специально предназначены для реализации политики безопасности, другие могут влиять на безопасность посредственно, и, наконец, третьи могут вообще не быть задействованы в решении задач обеспечения безопасности. Множество всех компонентов первых двух типов называется комплексом средств защиты (КСЗ).

Другими словами, КСЗ – это совокупность всех программно-аппаратных средств задействованных для реализации политики безопасности.

Под политикой безопасности необходимо понимать набор законов, правил, ограничений, рекомендаций и т.п., которые регламентируют порядок обработки информации и направленные на защиту информации от определенных угроз.

Под несанкционированным доступом (НСД) следует понимать доступ к информации с использованием средств, включенных в состав компьютерной

системы (КС), что нарушает правила разграничения доступа (ПРД). НСД может осуществляться как с использованием штатных средств, то есть совокупности программно-аппаратного обеспечения, включенного в состав КС разработчиком во время разработки или системным администратором в процессе эксплуатации, с включением в утвержденную конфигурацию КС, так и с использованием программно-аппаратных средств, включенных в состав КС преступником.

К основным способам НСД относятся:

- непосредственное обращение к объекту с целью получения определенного вида доступа;
- создание программно-аппаратных средств, которые выполняют обращение к объекту в обход средств защиты;
- модификация средств защиты, которая позволяет осуществление НСД;
- включение в КС программных или аппаратных механизмов, которые нарушают структуру и функции КС и позволяет осуществление НСД.

Под защитой от НСД следует понимать деятельность, направленную на обеспечение правил разграничения доступа путем создания и поддержания в рабочем состоянии системы мер по защите информации.

Для обеспечения безопасности информации во время ее обработки в системах создается комплексная система защиты информации (КСЗИ), процесс управления которой должен поддерживаться на протяжении всего жизненного цикла системы.

Согласно «Временному положению о категорировании объектов» категорированию подлежат объекты, в которых обсуждается, имеется, пересылается, принимается, преобразуется, накапливается, обрабатывается, отображается и сохраняется (т.е. циркулирует) информация с ограниченным доступом.

К объектам, которые подлежат категорированию, относятся:

- информационные, телекоммуникационные и информационно-телекоммуникационные системы и средства вычислительной техники;
- технические средства, которые предназначены для работы с информацией с ограниченным доступом, не относятся к информационно-телекоммуникационным системам, за исключением тех, которые основаны на криптографических методах защиты;
- помещения, предназначенные для проведения совещаний, конференций с использованием информации с ограниченным доступом;
- помещения, в которых расположены информационные, телекоммуникационные, информационно-телекоммуникационные системы и средства вычислительной техники, другие технические средства, предназначенные для работы с информацией с ограниченным доступом, в том числе и с использованием криптографических методов защиты.

Категорирование проводится с целью применения обоснованных методов технической защиты информации с ограниченным доступом, которая циркулирует на объектах, от утечки каналом побочных электромагнитных излучений и наводок, а также акустических (виброакустических) преобразований.

Устанавливаются четыре категории объектов в зависимости от режима доступа к информации, циркулирующей в них:

- к первой категории относятся объекты, в которых циркулирует информация, содержащая сведения, составляющие государственную тайну, для которой установлен гриф секретности «особой важности»;

- ко второй категории относятся объекты, в которых циркулирует информация, содержащая сведения, составляющие государственную тайну, для которой установлен гриф секретности «совершенно секретно»;

- к третьей категории относятся объекты, в которых циркулирует информация, содержащая сведения, составляющие государственную тайну, для которой установлен гриф секретности «секретно», а также информация, которая содержит сведения, составляющие другую предусмотренную законом (коммерческую, банковскую и т.д.) тайну, разглашение которой наносит ущерб личности, обществу и государству;

- к четвертой категории относятся объекты, в которых циркулирует служебная и конфиденциальная информация.

Ответственность за проведение работ по категорированию объектов несут руководители предприятий, учреждений, организаций всех форм собственности, воинских частей и формирований, субъектов властных полномочий, в ведении которых находятся соответствующие объекты.

Для проведения работ по категорированию объектов приказом руководителя организации назначается комиссия, которая определяет наивысший гриф секретности информации, которая циркулирует на объекте, а также основание для категорирования (первичное, плановое, в связи с изменениями грифа секретности). По результатам работы комиссии составляется акт, в котором приводятся указанные сведения, ранее установленная категория и приятое решение по категорированию.

Согласно НД ТЗИ 2.5-005-99 «Классификация автоматизированных систем и стандартные функциональные профили защищенности обрабатываемой информации от несанкционированного доступа», по совокупности характеристик системы делятся на три класса, требования к функциональному составу комплексных средств защиты которых существенно отличаются:

- класс «1» - одномашинный однопользовательский комплекс;

- класс «2» - локализованный многомашинный многопользовательский комплекс;

- класс «3» - разделенный многомашинный многопользовательский комплекс, в котором передача информации осуществляется через незащищенную среду (локальную сеть).

В рамках каждого класса системы классифицируются на основе требований по обеспечению определенных свойств информации. С точки зрения безопасности информация характеризуется тремя свойствами: конфиден-циальностью, целостностью и доступностью. В связи с этим, в каждом классе систем выделяются также подклассы:

- система, в которой повышенные требования к - обеспечению конфиденциальности обрабатываемой информации (подкласс «х.К»);

- система, в которой повышенные требования к - обеспечению целостности обрабатываемой информации (подкласс «х.Ц»);

- система, в которой повышенные требования к - обеспечению доступности обрабатываемой информации (подкласс «х.Д»);

- система, в которой повышенные требования к - обеспечению конфиденциальности и целостности обрабатываемой информации (подкласс «х.КЦ»);

- система, в которой повышенные требования к - обеспечению конфиденциальности и доступности обрабатываемой информации (подкласс «х.КД»);

- система, в которой повышенные требования к - обеспечению целостности и доступности обрабатываемой информации (подкласс «х.ЦД»);

- система, в которой повышенные требования к - обеспечению конфиденциальности, целостности и доступности обрабатываемой информации (подкласс «х.КЦД»).

Для каждого из подклассов каждого класса вводится некоторое количество иерархических стандартных функциональных профилей, которое может быть различным для каждого класса и подкласса систем.

Стандартный функциональный профиль защищенности представляет собой перечень минимально необходимых уровней услуг, которые должны реализовать комплексы средств защиты системы с целью удовлетворения определенных требований по защищенности информации, обрабатываемой в данной системе.

Стандартные функциональные профили строятся на основе существующих требований по защите информации от определенных угроз. При создании новых профилей, необходимо соблюдать требования НД ТЗИ 2.5-004-99 «Критерии оценки защищенности информации в компьютерных системах от несанкционированного доступа» (далее – Критерии). Этот нормативный документ устанавливает критерии оценки защищенности информации, обрабатываемой в информационных, коммуникационных, информационно-коммуникационных системах от несанкционированного доступа.

Критерии являются методологической базой для определения требований по защите информации в системах от несанкционированного доступа; создания защищенных компьютерных систем и средств защиты от несанкционированного доступа; оценки защищенности информации в системах и их пригодность для обработки информации с ограниченным доступом.

В процессе оценки возможности систем обеспечивать защиту обрабатываемой информации от несанкционированного доступа рассматриваются требования двух видов:

- требования к функции защиты;

- требования к гарантии.

В контексте Критериев система рассматривается как набор функциональных услуг. Каждая услуга представляет собой набор функций, позволяющих противостоять определенной угрозе. Каждая услуга может включать несколько уровней. Чем выше уровень услуги, тем более полно обеспечивается защита от определенного вида угроз.

Функциональные критерии разбиты на четыре группы, каждая из которых описывает требования к услугам, которые обеспечивают защиту от угроз одного из четырех типов:

- критерии конфиденциальности;
- критерии целостности;
- критерии доступности;
- критерии наблюдательности.

Кроме функциональных критериев, которые позволяют оценить наличие услуг безопасности в системе, Критерии содержат критерии гарантий, что позволяет оценить корректность реализации услуг. Критерии гарантий содержат семь уровней, которые являются иерархичными.

Таким образом, функциональный профиль защищенности информации в конкретной информационной, телекоммуникационной, информационно-телекоммуникационной системе может быть определен в результате проведения анализа угроз и оценки рисков или выбранный на основе класса системы в соответствии с НД ТЗИ 2.5-005-99 «Классификация автоматизированных систем и стандартные функциональные профили защищенности обрабатываемой информации от несанкционированного доступа».

Требования к защищенности информации от утечки по техническим каналам определяются на основании НД ТЗИ ВР ЭВТ-95 «Временные рекомендации по технической защите информации в средствах вычислительной техники, автоматизированных системах и сетях от утечки по каналам побочных электромагнитных излучений и наводок» и НД ТЗИ ВР ТЗИ ПЭМИН-95 «Временные рекомендации по технической защите информации от утечки по каналам побочных электромагнитных излучений и наводок».

2.2 Организация защиты информации в информационных, телекоммуникационных и информационно-телекоммуникационных системах

С целью защиты информации в информационных, телекоммуникационных, информационно-телекоммуникационных системах (ИТС) в государственных органах, на предприятиях, в учреждениях и организациях всех форм собственности создаются службы защиты информации (СЗИ).

Нормативный документ системы технической защиты информации – НД ТЗИ 1.4-001-2000 определяет требования к структуре и содержанию «Положения о службе защиты информации в автоматизированной системе».

Использование этого НД ТЗИ создает условия для внедрения единого подхода по определению и формированию задач, функций, структуры, полномочий службы защиты информации, а также организации работ по защите информации в продолжение всего жизненного цикла информационных, телекоммуникационных, информационно-телекоммуникационных систем в государственных органах, на предприятиях, в учреждениях и организациях всех форм собственности.

Целью этого НД ТЗИ является предоставление организациям, которые владеют, пользуются, распоряжаются информацией, подлежащей защите согласно нормативно-правовым актам, нормативно-методологической базы для разработки «Положения о службе защиты информации в автоматизированной системе» (далее - Положение).

Этот НД ТЗИ предусматривает при разработке Положения учет специфики деятельности организации, в информационно–телекоммуникационной системе (ИТС), которой создается и функционирует служба защиты информации, объема обработки информации, установленных в организации требований к конфиденциальности, целостности и доступности обрабатываемой информации, а также особенности технологии ее обработки.

При разработке Положения используются только те положения этого НД ТЗИ, которые соответствуют требованиям и условиям, характерным для данной организации (ИТС).

В общем случае Положение должно состоять из следующих разделов:

- общие положения;
- задачи службы защиты информации;
- функции службы защиты информации;
- полномочия и ответственность службы защиты информации;
- взаимодействие службы защиты информации с другими подразделениями организации и внешними предприятиями, учреждениями, организациями;
- штатное расписание и структура службы защиты информации;
- организация работ службы защиты информации;
- финансирование службы защиты информации.

Положение должно быть согласовано с юрисконсультом и руководителями подразделений (службы безопасности, режимно-секретные органы, подразделения ТЗИ) организации.

Положение утверждается приказом руководителя организации или подразделения, к которому структурно входит СЗИ.

Изменения существенного характера вносятся в Положение на основании распоряжения или приказа руководителя организации (подразделения, к которому структурно входит СЗИ).

Положение является нормативным документом организации (ИТС) и определяет задачи, функции, штатную структуру СЗИ, полномочия и ответственность сотрудников службы, взаимодействие с другими подразделениями организации и внешними организациями.

Служба защиты информации может быть штатным подразделением организации (ИТС) или внештатным подразделением организации (ИТС), самостоятельным структурным подразделением с непосредственной подчиненностью руководителю (заместителю руководителя) организации или структурной единицей (подразделения ТЗИ, службы безопасности) организации.

В организациях, где штатным расписанием не предусмотрено создание СЗИ, меры по обеспечению защиты информации в ИТС осуществляют назначенные приказом руководителя организации работники. В этом случае должностные (функциональные) обязанности этих работников должны включать положения,

предусматривающие выполнение ими требований относительно деятельности СЗИ.

Целью создания СЗИ является организационное обеспечение задач управления комплексной системой защиты информации (КСЗИ) в ИТС и осуществления контроля за ее функционированием. На СЗИ возлагается выполнение работ по определению требований по защите информации в ИТС, проектированию, разработке и модернизации КСЗИ, а также по эксплуатации, обслуживанию, поддержке работоспособности КСЗИ, контролю за состоянием защищенности информации в ИТС.

В своей работе СЗИ взаимодействует с подразделениями организации (режимно-секретными органами, службой безопасности, подразделением ТЗИ и др.), а также с государственными органами, учреждениями и организациями, занимающимися вопросами защиты информации.

В случае необходимости, к выполнению работ могут привлекаться внешние организации, имеющие лицензии на соответствующий вид деятельности в сфере защиты информации.

Задачи СЗИ:

- защита законных прав безопасности информации организации, отдельных ее структурных подразделений, персонала в процессе информационной деятельности и взаимодействия между собой, а также во взаимоотношениях с внешними отечественными и зарубежными организациями;
- исследование технологии обработки информации в ИТС с целью выявления возможных каналов утечки и других угроз безопасности информации, формирование модели угроз, разработки политики безопасности информации, определение мер, направленных на ее реализацию;
- организация и координация работ, связанных с защитой информации в ИТС, необходимость защиты которой определяется ее собственником или действующим законодательством, поддержание необходимого уровня защищенности информации, ресурсов и технологий;
- разработка проектов нормативных и распорядительных документов, действующих в рамках организации, согласно которым должна обеспечиваться защита информации в ИТС;
- организация работ по созданию и использованию КСЗИ на всех этапах жизненного цикла ИТС;
- участие в организации профессиональной подготовки и повышении квалификации персонала и пользователей ИТС по вопросам защиты информации;
- формирование у персонала и пользователей понимания необходимости выполнения требований нормативно-правовых актов, нормативных и распорядительных документов, касающихся сферы защиты информации;
- организация обеспечения выполнения персоналом и пользователями требований нормативно-правовых актов, нормативных и распорядительных документов по защите информации в ИТС и проведения контрольных проверок их выполнения.

Функции службы защиты информации:

- определение перечней сведений, подлежащих защите в процессе обработки, других объектов защиты в ИТС, классификация информации по требованиям к ее конфиденциальности или важности для организации, необходимым уровням защищенности информации, определение порядка ввода (вывода), использование и распоряжение информацией в ИТС;

- разработка и корректировка модели угроз и модели защиты информации в ИТС, политики безопасности информации в ИТС;

- определение и формирование требований к КСЗИ;

- организация и координация работ по проектированию и разработке КСЗИ, непосредственное участие в проектных работах по созданию КСЗИ;

- подготовка технических предложений, рекомендаций по предотвращению утечки информации по техническим каналам и предупреждения попыток несанкционированного доступа к информации при создании КСЗИ;

- организация работ и участие в испытаниях КСЗИ, проведении ее экспертизы;

- выбор организаций-исполнителей работ по созданию КСЗИ, осуществление контроля за соблюдением установленного порядка проведения работ по защите информации, во взаимодействии с подразделением ТЗИ (режимно-секретными органами, службой безопасности организации) согласование основных технических и распорядительных документов, сопровождающих процесс создания КСЗИ (техническое задание, технический и рабочий проекты, программа и методика испытаний, планы работ и др.);

- участие в разработке нормативных документов, действующих в рамках организации и ИТС, которые устанавливают административную ответственность за нарушение требований по безопасности информации и установленных правил эксплуатации КСЗИ;

- участие в разработке нормативных документов, действующих в рамках организации и ИТС, которые устанавливают правила доступа пользователей к ресурсам ИТС, определяющие порядок, нормы, правила по защите информации и осуществления контроля за их соблюдением (инструкций, положений, приказов, рекомендаций и др.);

- организация процесса управления КСЗИ;

- расследование случаев нарушения политики безопасности, опасных и непредвиденных событий, осуществление анализа причин, приведших к ним, сопровождение банка данных таких событий;

- принятие мер в случае выявления попыток НСД к ресурсам ИТС, нарушении правил эксплуатации средств защиты информации или других дестабилизирующих факторов;

- обеспечение контроля целостности средств защиты информации и быстрое реагирование на их выход из строя или нарушения режимов функционирования;

- организация управления доступом к ресурсам ИТС (распределение между пользователями необходимых реквизитов защиты информации - паролей, привилегий, ключей и др.);

- сопровождение и актуализация базы данных защиты информации (матрицы доступа, классификационные метки объектов, идентификаторы пользователей и т.д.);

- наблюдение (регистрация и аудит событий в ИТС, мониторинг событий и т.п.) за функционированием КСЗИ и ее компонентов;

- подготовка предложений по совершенствованию порядка обеспечения защиты информации в ИТС, внедрение новых технологий защиты и модернизации КСЗИ;

- организация и проведение мероприятий по модернизации, тестированию, оперативного восстановления функционирования КСЗИ после сбоев, отказов, аварий ИТС или КСЗИ;

- участие в работах по модернизации ИТС - согласовании предложений по введению в состав ИТС новых компонентов, новых функциональных задач и режимов обработки информации, замены средств обработки информации и т.п.;

- обеспечение сопровождения и актуализации эталонных, архивных и резервных копий программных компонентов КСЗИ, обеспечение их хранения и тестирования;

- проведение аналитической оценки текущего состояния безопасности информации в ИТС (прогнозирование возникновения новых угроз и их учета в модели угроз, определение необходимости ее корректировки, анализ соответствия технологии обработки информации и реализуемой политики безопасности текущей модели угроз и др.);

- информирование собственников информации о технических возможностях защиты информации в ИТС и типовые правила, установленные для персонала и пользователей ИТС;

- немедленное вмешательство в процесс работы ИТС в случае обнаружения атаки на КСЗИ, проведение в таких случаях работ по разоблачению нарушителя;

- регулярное представление отчетов руководству организации-владельца (распорядителя) ИТС о выполнении пользователями ИТС требований по защите информации;

- анализ сведений о технических средствах защиты информации нового поколения, обоснование предложений по приобретению средств для организации;

- контроль за выполнением персоналом и пользователями ИТС требований, норм, правил, инструкций по защите информации в соответствии с определенной политикой безопасности информации, в том числе контроль за обеспечением режима секретности в случае обработки в ИТС информации, составляющей государственную тайну;

- контроль за обеспечением охраны и порядка хранения документов (носителей информации), содержащих сведения, подлежащие защите;

- разработка и реализация совместно с РСО (подразделением ТЗИ, службой безопасности) организации комплексных мер по безопасности информации при проведении мероприятий научно-технического, экономического, информационного сотрудничества с иностранными фирмами, а также при проведении совещаний, переговоров и др., осуществление их технического и информационного обеспечения.

Права, обязанности и ответственность службы защиты информации

Служба защиты информации имеет право:

- осуществлять контроль за деятельностью любого структурного подразделения организации (ИТС) о выполнении им требований нормативно-правовых актов и нормативных документов по защите информации;

- представлять руководству организации предложения о приостановлении процесса обработки информации, запрета обработки, изменения режимов обработки и т.д. в случае выявления нарушений политики безопасности или в случае возникновения реальной угрозы нарушения безопасности;

- составлять и представлять руководству организации акты по выявленным нарушениям политики безопасности, готовить рекомендации по их устранению;

- проводить служебные расследования в случаях выявления нарушений;

- получать доступ к работам и документов структурных подразделений организации (ИТС), необходимых для оценки принятых мер по защите информации и подготовки предложений по их дальнейшему совершенствованию;

- готовить предложения по привлечению на договорной основе к выполнению работ по защите информации других организаций, имеющих лицензии на соответствующий вид деятельности;

- готовить предложения по обеспечению ИТС (КСЗИ) необходимыми техническими и программными средствами защиты информации и другой специальной техникой, которые разрешены для использования в Украине с целью обеспечения защиты информации;

- выходить к руководству организации с предложениями относительно подачи заявлений в соответствующие государственные органы на проведение государственной экспертизы КСЗИ или сертификации отдельных средств защиты информации;

- согласовывать условия включения в состав ИТС новых компонентов и представлять руководству предложения о запрете их включения, если они нарушают принятую политику безопасности или уровень защищенности ресурсов ИТС;

- давать заключения по вопросам, относящимся к компетенции СЗИ, которые необходимы для осуществления производственной деятельности организации, особенно технологий, доступ к которым ограничен, других проектов, требующих поддержки со стороны сотрудников СЗИ;

- выходить к руководству организации с предложениями по согласованию планов и регламента посещения ИТС посторонними лицами;

- другие права, предоставленные СЗИ в соответствии со спецификой и особенностями деятельности организации (ИТС).

Служба защиты информации обязана:

- организовать обеспечение полноты и качественного выполнения организационно-технических мероприятий по защите информации в ИТС;

- своевременно и в полном объеме доводить до пользователей и персонала ИТС информацию об изменениях в области защиты информации, которые их касаются;

- проверять соответствие принятых в ИТС (организации) правил, инструкций по обработке информации, осуществлять контроль за выполнением этих требований;

- осуществлять контрольные проверки состояния защищенности информации в ИТС;

- обеспечивать конфиденциальность работ по монтажу, эксплуатации и технического обслуживания средств защиты информации, установленных в ИТС (организации);

- содействовать и, в случае необходимости, принимать непосредственное участие в проведении высшими органами проверок состояния защищенности информации в ИТС;

- способствовать (техническими и организационными мероприятиями) созданию и соблюдению условий хранения информации, полученной организацией на договорных, контрактных или иных основаниях от организаций-партнеров, поставщиков, клиентов и частных лиц;

- периодически, не реже одного раза в месяц (иной срок), представлять руководству организации отчет о состоянии защищенности информации в ИТС и соблюдения пользователями и персоналом ИТС установленного порядка и правил защиты информации;

- немедленно сообщать руководству ИТС (организации) о выявленных атаки и разоблаченных нарушителей;

- другие обязанности, возложенные на руководителя и сотрудников СЗИ в соответствии со спецификой и особенностями деятельности ИТС (организации).

Ответственность службы защиты информации

Руководство и сотрудники СЗИ за неисполнение или ненадлежащее исполнение служебных обязанностей, допущенные ими нарушения установленного порядка защиты информации в ИТС несут дисциплинарную, административную, гражданско-правовую, уголовную ответственность согласно законодательству Украины.

Персональная ответственность руководителя и сотрудников СЗИ определяется должностными (функциональными) инструкциями.

Ответственность за деятельность СЗИ возлагается на его руководителя.

Руководитель СЗИ отвечает за:

- организацию работ по защите информации в ИТС, эффективность защиты информации в соответствии с действующими нормативно-правовыми актами;

- своевременная разработка и выполнение «Плана защиты информации в автоматизированной системе»;

- качественное выполнение сотрудниками СЗИ задач, функций и обязанностей, указанных в Положении, должностных инструкциях, а также плановых мероприятий по защите информации, утвержденных руководителем организации;

- координацию планов деятельности подразделений и служб ИТС (организации) по вопросам защиты информации;

- создание системы обучения сотрудников, пользователей, персонала ИТС по вопросам защиты информации;

- выполнение лично и сотрудниками СЗИ распоряжений руководителя организации, правил внутреннего трудового распорядка, установленного режима, правил охраны труда и противопожарной охраны.

Сотрудники СЗИ отвечают за:

- соблюдение требований нормативных документов, определяющих порядок организации работ по защите информации, информационных ресурсов и технологий;

- полноту и качество разработки и внедрения организационно-технических мероприятий по защите информации в ИТС, точность и достоверность полученных результатов и выводов по вопросам, относящимся к компетенции СЗИ;

- соблюдение сроков проведения контрольных, инспекционных, проверочных и других мероприятий по оценке состояния защищенности информации в ИТС, которые включены в план работ СЗИ;

- качество и правомерность документального оформления результатов работ отдельных этапов создания КСЗИ, документального оформления результатов проверок;

- другие вопросы персональной ответственности, которые возложены на руководителя и сотрудников СЗИ в соответствии со спецификой и особенностями деятельности ИТС (организации).

Взаимодействие службы защиты информации с другими подразделениями организации и внешними организациями

СЗИ осуществляет свою деятельность во взаимодействии с научными, производственными и другими организациями, государственными органами и учреждениями, занимающимися вопросами защиты информации.

Мероприятия по защите информации в ИТС должны быть согласованы СЗИ с мерами охранной и режимно-секретной деятельности других подразделений организации.

СЗИ взаимодействует, согласовывает свою деятельность и устанавливает связи с:

- режимно-секретными органами организации;

- подразделением ТЗИ организации;

- администрацией ИТС и другими подразделениями организации, производственная деятельность которых связана с защитой информации или ее автоматизированной обработкой;

- службой безопасности организации;

- внешними организациями, которые являются партнерами, пользователями, поставщиками, исполнителями работ;

- подразделениями служб безопасности иностранных фирм (партнерами, пользователями, поставщиками, исполнителями работ), их представительствами (на договорных или иных началах);

- другими субъектами деятельности в области защиты информации.

2.3 Порядок проведения работ по созданию комплексной системы защиты информации в информационно-телекоммуникационной системе

Стремительное развитие информационных технологий и их внедрение во всех сферах деятельности значительно совершенствует и ускоряет многие бизнес-процессы. Наличие или отсутствие необходимой информации, ее сохранность и защищенность от стороннего вмешательства существенно влияет на благополучие компании. Но с каждым годом все больше возрастает количество вирусов, сетевых атак злоумышленников, возникают угрозы нарушения конфиденциальности информации внутри компании, что приводит к финансовым потерям, и часто - весьма значительным. Решение вопросов защиты данных в современных информационных системах будет успешным только при условии использования комплексного подхода к построению системы обеспечения безопасности информации.

Комплексная система защиты информации (КСЗИ) - совокупность организационных и инженерно-технических мероприятий, которые направлены на обеспечение защиты информации от разглашения, утечки и несанкционированного доступа.

Организационные мероприятия являются обязательной составляющей построения любой КСЗИ. Инженерно-технические мероприятия осуществляются по мере необходимости.

Организационные мероприятия включают в себя создание концепции информационной безопасности, а также:

- составление должностных инструкций для пользователей и обслуживающего персонала;
- создание правил администрирования компонент информационной системы, учета, хранения, размножения, уничтожения носителей информации, идентификации пользователей;
- разработка планов действий в случае выявления попыток несанкционированного доступа к информационным ресурсам системы, выхода из строя средств защиты, возникновения чрезвычайной ситуации;
- обучение правилам информационной безопасности пользователей.

В случае необходимости, в рамках проведения организационных мероприятий может быть создана служба информационной безопасности, проведена реорганизация системы делопроизводства и хранения документов.

Инженерно-технические мероприятия - совокупность специальных технических средств и их использование для защиты информации. Выбор инженерно-технических мероприятий зависит от уровня защищенности информации, который необходимо обеспечить.

Инженерно-технические мероприятия, проводимые для защиты информационной инфраструктуры организации, могут включать использование защищенных подключений, межсетевых экранов, разграничение потоков информации между сегментами сети, использование средств шифрования и защиты от несанкционированного доступа.

В случае необходимости, в рамках проведения инженерно-технических мероприятий, может осуществляться установка в помещениях систем охранно-пожарной сигнализации, систем контроля и управления доступом.

Отдельные помещения могут быть оборудованы средствами защиты от утечки акустической (речевой) информации.

В процесс создания КСЗИ вовлекаются следующие стороны (субъекты КСЗИ):

- организация, для которой осуществляется построение КСЗИ (Заказчик);
- организация, осуществляющая мероприятия по построению КСЗИ (Исполнитель);
- Государственная служба специальной связи и защиты информации Украины (ГСССЗИУ) (Контролирующий орган);
- организация, осуществляющая государственную экспертизу КСЗИ (Организатор экспертизы);
- организация, в случае необходимости привлекаемая Заказчиком или Исполнителем для выполнения некоторых работ по созданию КСЗИ (Подрядчик).

Объектами защиты КСЗИ является информация, в любом ее виде и форме представления.

В зависимости от вида и формы представления информационных сигналов, которые циркулируют в информационно-телекоммуникационной системе (ИТС), в том числе и в автоматизированных системах (АС), при построении КСЗИ могут использоваться различные средства защиты.

Таким образом, КСЗИ могут быть созданы для АС всех классов:

- одномашинных пользовательских комплексов (АС класса 1);
- локализованных многомашинных многопользовательских комплексов (АС класса 2);
- распределенных многомашинных многопользовательских комплексов (АС класса 3).

Деятельность по созданию КСЗИ относится к лицензируемым видам деятельности и лицензируется Государственной службой специальной связи и защиты информации Украины.

Право на проведение государственных экспертиз КСЗИ имеют лицензиаты в области ТЗИ, которые также входят в Реестр Организаторов государственной экспертизы в сфере ТЗИ, который формирует и ведет Контролирующий орган.

Необходимость построения КСЗИ определяется требованиями нормативных документов или желанием владельца информационных ресурсов.

Согласно Закону Украины «О защите информации в информационно-телекоммуникационных системах»:

- информация, которая принадлежит к государственным информационным ресурсам, или информация с ограниченным доступом должна быть защищена путём построения КСЗИ, с получением «Аттестата соответствия», который выдаётся ГСССЗИУ;
- прочая информация может быть защищена с помощью КСЗИ по желанию её владельца.

Порядок проведения работ по созданию комплексной системы защиты информации в информационных, телекоммуникационных, информационно-телекоммуникационных системах (ИТС) определяется нормативным документом технической защиты информации НД ТЗИ 3.7-003-05. Этот документ определяет основы организации и порядок выполнения работ по защите информации в ИТС, порядок принятия решения по составу комплексной защиты информации в зависимости от условий функционирования ИТС и видов обрабатываемой информации, определения объема и содержания работ, этапности работ, основных заданий и порядка выполнения работ по каждому этапу.

Порядок создания КСЗИ в ИТС является единым независимо от того, создается КСЗИ в ИТС, которая проектируется или для действующей ИТС, или возникла необходимость обеспечения защиты информации или модернизации уже созданной КСЗИ.

Процесс создания КСЗИ заключается в осуществлении комплекса взаимосогласованных мер, направленных на разработку и внедрение информационных технологии, которые обеспечивают обработку информации в ИТС согласно с требованиями, установленными нормативно-правовыми актами и нормативными документами в сфере защиты информации.

В состав КСЗИ входят мероприятия и средства, которые реализуют способы, методы, механизмы защиты информации от:

- утечки по техническим каналам, к которым относятся каналы побочных электромагнитных излучений и наводок, акустоэлектрические и другие каналы;
- несанкционированных действий и несанкционированного доступа к информации, которые могут осуществляться путем подключения к аппаратуре и линиям связи, маскировка под зарегистрированного пользователя, преодоления мер защиты с целью использования информации или навязывания ложной информации, применения закладных устройств или программ, использование компьютерных вирусов и др.;
- специального воздействия на информацию, которое может осуществляться путем формирования полей и сигналов с целью нарушения целостности информации или разрушению системы защиты.

Для каждой конкретной ИТС состав, структура и требования к КСЗИ определяются свойствами обрабатываемой информации, классом автоматизированной системы и условиями эксплуатации ИТС.

В случаях, определенных законодательством, работы по проектированию, разработке, изготовлению, испытанию, эксплуатации ИТС должны выполняться в комплексе с мерами, по обеспечению режима секретности, противодействию техническим разведкам, а также с режимными мерами по охране информации с ограниченным доступом, которая не является государственной тайной.

Создание комплексов технической защиты информации от утечки по техническим каналам осуществляется, если в ИТС обрабатывается информация, составляющая государственную тайну, или когда необходимость этого определены собственником информации.

Создание комплекса средств защиты (КСЗ) от НСД осуществляется во всех ИТС, где обрабатывается информация, которая принадлежит к государственным

информационным ресурсам, относится к государственной или иной тайне или к отдельным видам информации, необходимость защиты которой определена законодательством, а также в ИТС, где такая необходимость определена владельцем информации.

Порядок создания, внедрения, сопровождения и модернизации средств технической защиты информации от несанкционированного доступа определяется НД ТЗИ 3.6-001-2000.

Средство технической защиты информации от НСД – это программное, аппаратное или программно-аппаратное средство, которое создается как отдельный продукт производства, имеет необходимую программную и/или конструкторскую документацию и обеспечивает самостоятельно или в комплексе с другими средствами защиту от угроз НСД для информации в компьютерных системах, или используется для контроля эффективности защиты информации от НСД в таких системах.

Защищенный от НСД компонент вычислительной системы – это программное, аппаратное или программно-аппаратное средство, у которого, дополнительно к основному предназначению, предусмотрены функции защиты информации от угроз НСД.

Решение о необходимости принятия мер защиты от специальных воздействий на информацию принимается владельцем информации в каждом случае отдельно.

Работы по созданию КСЗИ выполняются организацией-владельцем (распорядителем) ИТС с соблюдением требований нормативно-правовых актов относительно осуществления деятельности в области защиты информации. В зависимости от состава КСЗИ может оказаться, что для ее создания необходимо выполнять несколько различных видов работ, подлежащих лицензированию в рамках хозяйственной деятельности (получение разрешения) по технической защите информации. В этом случае разработчик КСЗИ должен иметь право на осуществление хотя бы одного из следующих видов работ. Для выполнения работ, на осуществление которых разработчик КСЗИ не имеет лицензии (разрешения), привлекаются соисполнители, которые имеют соответствующие лицензии.

Для организации работ по созданию КСЗИ в ИТС создается служба защиты информации, порядок создания, задачи, функции, структура и полномочия которого определены в НД ТЗИ 1.4-001-2000.

СЗИ создается после принятия решения о необходимости создания КСЗИ. Как исключение СЗИ может создаваться на более поздних этапах работ, но не позднее этапа подготовки КСЗИ до введения в действие.

Существует несколько этапов создания комплексной системы защиты информации в информационных, телекоммуникационных и информационно-телекоммуникационных системах. Такими этапами являются:

- обоснование необходимости создания КСЗИ;
- обследование среды функционирования ИТС;
- формирование задач по созданию КСЗИ.

Обоснование необходимости создания КСЗИ

Основанием для определения необходимости создания КСЗИ являются нормы и требования действующего законодательства, которые устанавливают обязательность ограничения доступа к определенным видам информации, обеспечивают ее целостность или доступность, а также принятое собственником решение по этому вопросу, если нормативно-правовые акты дают ему право действовать на собственный рассудок.

Исходными данными для обоснования необходимости создания КСЗИ в общем случае являются результаты:

- анализа нормативно-правовых актов (государственных, ведомственных и таких, которые действуют в пределах учреждений, организаций, предприятий) на основании которых может устанавливаться ограничение доступа к определенным видам информации, запрет на такого вида ограничения или определяться в необходимости обеспечения защиты информации согласно других критериев;

- определение наличия в составе информации, которая подлежит автоматизированной обработке , таких ее видов, которые потребуют ограничения доступа к ней или обеспечение целостности или доступности в соответствии с требованиями нормативно-правовых актов;

- оценка возможных преимуществ (финансово-экономических, социальных и т.п.) эксплуатации ИТС в случае создания КСЗИ.

На основании проведенного анализа принимается решение о необходимости создания КСЗИ.

Обследование среды функционирования ИТС

В процессе обследования среды функционирования ИТС рассматривается как организационно-техническая система, которая объединяет вычислительную систему, физическую среду, среду пользователей, обрабатываемую информацию и технологию ее обработки (среда функционирования ИТС).

Целью обследования является подготовка исходных данных для формирования требований к КСЗИ в виде описания каждой среды функционирования ИТС и выявления в ней элементов, которые непосредственно или опосредованно могут влиять на безопасность информации, выявления взаимного влияния элементов различных сред, документирования результатов обследования для использования на следующих этапах работ.

Обследование выполняется, когда разработана концепция ИТС (основные принципы и подходы построения), определены основные задачи и характеристики ИТС, функциональных комплексов ИТС и существует вариант (ы) их реализации.

При обследовании вычислительной системы ИТС должны быть проанализированы и описаны:

- общая структурная схема и состав (перечень и состав оборудования, технических и программных средств, их связи, особенности конфигурации, архитектуры и топологии, программные и программно-аппаратные средства защиты информации, взаимное расположение средств и т.п.);

- виды и характеристики каналов связи;

- особенности взаимодействия отдельных компонентов, их взаимное влияние друг на друга;

- возможные ограничения на использование средств и др.

Должны быть выявлены компоненты вычислительной системы, содержащие и не содержащие средства и механизмы защиты информации, потенциальные возможности этих средств и механизмов, их свойства и характеристики, в том числе, устанавливаемые по умолчанию и др.

Целью такого анализа является получение общего представления о наличии потенциальных возможностей по обеспечению защиты информации, выявление компонентов ИТС, которые требуют повышенных требований к защите информации и внедрения дополнительных мер защиты.

При обследовании информационной среды анализу подлежит вся информация, которая обрабатывается, а также сохраняется в ИТС (данные и программное обеспечение). При анализе информация должна быть классифицирована по режиму доступа, за правовым режимом, определены и описаны виды (в терминах объектов КС) ее представления в ИТС.

Для каждого вида информации и типа объекта, в котором она содержится, ставятся в соответствие свойства защищенности информации (конфиденциальность, целостность, доступность) или КС (наблюдаемость), которым они должны соответствовать.

Анализ технологии обработки информации должен выявить особенности обращения электронных документов, должны быть определены и описаны информационные потоки и среды, через которые они передаются, источники образования потоков и места их назначения, принципы и методы управления информационными потоками, составлены структурные схемы потоков. Фиксируются виды носителей информации и порядок их использования во время функционирования ИТС.

Для каждого структурного элемента схемы информационных потоков фиксируются состав информационных объектов, режим доступа к ним, возможное влияние на него (элемента) элементов среды пользователей, физической среды с точки зрения сохранения свойств информации.

При обследовании физической среды осуществляется анализ взаимного расположения средств обработки информации ИТС на объектах информационной деятельности, коммуникаций, систем жизнеобеспечения и связи, а также режим функционирования этих объектов.

Порядок проведения обследования должен соответствовать ДСТУ 3396.1.

Анализу подлежат следующие характеристики физической среды:

- территориальное размещение компонентов ИТС (генеральный план, ситуационный план);
- наличие охраны территории и пропускной режим;
- наличие категорированных помещений, в которых должны размещаться компоненты ИТС;
- режим доступа к компонентам физической среды ИТС;
- воздействие факторов окружающей среды, защищенность от средств технической разведки;
- наличие элементов коммуникаций, систем жизнеобеспечения и связи, имеющих выход за пределы контролируемой зоны;
- наличие и характеристики систем заземления;

- условия хранения магнитных, оптико-магнитных, бумажных и других носителей информации;

- наличие проектной и эксплуатационной документации на компоненты физической среды.

При обследовании среды пользователей осуществляется анализ:

- функционального и количественного состава пользователей, их функциональных обязанностей и уровня квалификации;

- полномочий пользователей о допуске к сведениям, которые обрабатываются в ИТС, доступа к ИТС и ее отдельным компонентам;

- полномочий пользователей по управлению КСЗИ;

- уровня возможностей различных категорий пользователей;

- наличия СЗИ в ИТС.

Результаты обследования сред функционирования ИТС оформляются в виде акта и включаются, в случае необходимости, в соответствующие разделы плана защиты информации в ИТС (далее - План защиты), который разрабатывается согласно НД ТЗИ 1.4-001.

По результатам обследования сред функционирования ИТС утверждается перечень объектов защиты (с учетом рекомендаций НД ТЗИ 1.4-001, НД ТЗИ 2.5-007, НД ТЗИ 2.5-008, НД ТЗИ 2.5-010 по классификации объектов), а также определяются потенциальные угрозы для информации и разрабатываются модель угроз и модель нарушителя. Построение моделей осуществляется в соответствии с НД ТЗИ 1.1-002, НД ТЗИ 1.4-001 и НД ТЗИ 1.6-003. Модель угроз для информации и модель нарушителя рекомендуется оформлять в виде отдельных документов (или объединенных в один документ) - Плана защиты.

Формирование задания на создание КСЗИ

На этом этапе:

- определяются задачи защиты информации в ИТС, цель создания КСЗИ, вариант решения задач защиты (согласно ДСТУ 3396.1), основные направления обеспечения защиты;

- осуществляется анализ рисков (изучение модели угроз и модели нарушителя, возможных последствий от реализации потенциальных угроз, величины возможных убытков и др.) и определяется перечень существенных угроз;

- определяются общая структура и состав КСЗИ, требования к возможным мероприятиям, методам и средствам защиты информации, допустимые ограничения применения определенных мер и средств защиты (например, ограничения на использование средств активной защиты от утечки информации по каналам ПЭМИН за счет использования средств электронно-вычислительной техники в защищенном исполнении др.), другие ограничения сред функционирования ИТС, ограничения по использованию ресурсов ИТС для реализации задач защиты, допустимые расходы на создание КСЗИ, условия создания, введения в действие и функционирования КСЗИ (отдельных ее подсистем, компонентов), общие требования к соотношению и пределам применения в ИТС (отдельных ее подсистемах, компонентах) организационных,

инженерно-технических, технических, криптографических и других мер защиты информации, которые войдут в состав КСЗИ.

Осуществляется оформление отчета о выполнении работ на этой стадии и оформление заявки на разработку КСЗИ (тактико-технического задания на создание КСЗИ или другого документа аналогичного содержания, который его заменяет).

Разработка политики безопасности информации в ИТС

Разработка политики безопасности в информационных, телекоммуникационных и информационно-телекоммуникационных системах состоит из этапов:

- изучение объекта, на котором создается КСЗИ и проведение научно-исследовательских работ;
- выбор варианта КСЗИ;
- оформления политики безопасности.

На первом этапе проводится детальное изучение объекта, на котором создается КСЗИ, уточняются модели угроз, потенциальный нарушитель и результаты анализа возможностей управления рисками, которые выполнены на предыдущих этапах, а также выполняются, в случае необходимости, дополнительные научно-исследовательские работы, связанные с поиском путей реализации заданий по созданию КСЗИ, оформляются и утверждаются отчеты по НИР, которые исполнялись.

На втором этапе в общем случае по результатам работ предыдущего этапа готовятся альтернативные варианты концепции создания КСЗИ и планов их реализации, осуществляется оценка преимуществ и недостатков каждого из вариантов, выбор наиболее оптимального варианта. Концепция оформляется в виде отчета.

На третьем этапе осуществляется:

- выбор основных решений по противодействию всем существенным угрозам, формирование общих требований, правил, ограничений, рекомендаций и т.п., регламентирующих использование защищенных технологий обработки информации в ИТС, отдельных мероприятий и средств защиты информации, деятельность пользователей всех категорий;
- документальное оформление политики безопасности информации.

Политика безопасности может разрабатываться для ИТС в целом или, если имеют место особенности функционирования отдельных компонентов КСЗИ, для отдельной компоненты, для отдельной функциональной задачи, для отдельной технологии обработки информации и т.п.

Политика безопасности разрабатывается в соответствии с положениями НД ТЗИ 1.1-002 и рекомендациями НД ТЗИ 1.4-001. Политику безопасности рекомендуется оформлять в виде отдельного документа - Плана защиты.

Разработка технического задания на создание КСЗИ

ТЗ на создание КСЗИ в ИТС является основным организационно-техническим документом, который определяет требования по защите обрабатываемой в ИТС информации, порядок создания КСЗИ, порядок проведения всех видов испытаний КСЗИ и ввод ее в эксплуатацию в составе ИТС.

ТЗ на создание КСЗИ разрабатывается на соответствующей стадии работ по созданию ИТС на основе комплексного подхода к построению КСЗИ, который предусматривает объединение в единую систему всех необходимых мер и средств защиты от угроз безопасности информации на всех этапах жизненного цикла ИТС.

ТЗ на создание КСЗИ может разрабатываться для впервые создаваемых ИТС, а также при модернизации уже существующих ИТС.

Для оформления ТЗ на КСЗИ могут быть использованы следующие варианты:

- в виде отдельного раздела ТЗ на создание ИТС;
- в виде отдельного (частичного) ТЗ;
- в виде дополнения к ТЗ на создание ИТС.

Ограничений по выбору варианта не устанавливается.

Первый вариант рекомендуется применять для вновь созданных ИТС. Второй или третий варианты рекомендуется использовать в случае модернизации КСЗИ, модернизации действующих ИТС, а также для ИТС, которые уже имеют утвержденное ТЗ на создание, в котором не содержится отдельного раздела по защите информации.

Разработка проекта КСЗИ

Проект КСЗИ разрабатывается на основании и в соответствии с ТЗ на создание ИТС (дополнения к нему, отдельного ТЗ на создание КСЗИ).

При разработке проекта КСЗИ обосновываются и принимаются проектные решения, позволяющие реализовать требования ТЗ, обеспечить совместимость и взаимодействие различных компонентов КСЗИ, а также различных мероприятий и способов защиты информации.

Проект КСЗИ выполняется на таких стадиях создания ИТС: эскизный проект, технический проект, рабочий проект.

На стадии эскизного проекта:

1) осуществляется разработка предварительных проектных решений КСЗИ и, в случае необходимости, ее отдельных составных частей, а также разработка, оформление, согласование и утверждение документации на КСЗИ. Содержание и стиль документации должны быть достаточными для полного описания проектных решений уровня эскизного проекта;

2) определяются: функции КСЗИ в целом и функции ее отдельных составных частей; состав комплексов технической защиты информации от утечки по техническим каналам и от специальных воздействий; перечень мер противодействия техническим разведкам; перечень организационных, правовых и других мер защиты; составляющие КСЗ; обобщенная структура КСЗИ и схема взаимодействия составных частей;

3) предлагаются предварительные технические решения, с помощью которых предполагается реализация задач и функций КСЗИ.

На стадии технического проекта КСЗИ:

1) выполняется разработка: общих проектных решений, необходимых для реализации требований ТЗ на КСЗИ; решений по структуре КСЗИ (организационной структуры, структуры технических и программных средств),

алгоритмов функционирования и условий использования средств защиты; решений по архитектуре КСЗ и механизмов реализации, определенных функциональным профилем услуг безопасности информации.

Осуществляются организационно-технические мероприятия по обеспечению последовательности разработки КСЗ, архитектуры, среды разработки, испытаний, среды функционирования и эксплуатационной документации КСЗ в соответствии с заданным уровнем гарантий реализации услуг безопасности согласно со спецификациями НД ТЗИ 2.5-004, НД ТЗИ 2.5-007, НД ТЗИ 2.5-008, НД ТЗИ 2.5-010;

2) выполняется разработка, оформление, согласование и утверждение документации в объеме, предусмотренном ТЗ на КСЗИ. Содержание и стиль документации должны быть достаточными для полного описания проектных решений уровня технического проекта;

3) разработка документации на поставку средств защиты информации и/или технических требований (технических заданий) на их разработку.

Готовится и оформляется документация на поставку средств защиты или продукции, содержащей их в своем составе, для комплектации КСЗИ. Если необходимой продукции нет на рынке средств защиты, определяются технические требования (состоят технические задания) на разработку соответствующих средств;

4) осуществляется разработка, оформление и утверждение заданий на проектирование из смежных вопросов, связанных с созданием КСЗИ или влияют на условия ее функционирования (строительные, электротехнические, санитарно-технические и другие подготовительные работы).

На стадии рабочего проекта КСЗИ:

1) осуществляется разработка, оформление и утверждение рабочей и эксплуатационной документации КСЗИ и, в случае необходимости, ее отдельных составных частей.

Рабочая документация содержит подробные решения по реализации технического проекта КСЗИ, по обеспечению управления КСЗИ и взаимодействия ее компонентов, а также документацию, необходимую для тестирования, проведение пусконаладочных работ, проведения испытаний КСЗИ;

2) Проводится разработка средств защиты информации или адаптация готовой продукции к условиям функционирования КСЗИ. Разработка средств защиты информации от НСД осуществляется согласно НД ТЗИ 3.6-001.

В состав рабочей документации на комплексы технической защиты информации от утечки по техническим каналам должны входить схемы размещения основных технических средств (ОТС) ИТС, кабельного оборудования, сетей питания и систем заземления, которые выполняются в соответствии с требованиями нормативных документов ВР ЭВТ - 95, ВР ТЗИ-ПЭМИН- 95, СТР-2, СТР-3, СВТР-78. При этом учитываются условия их размещения и минимально допустимые расстояния между этими средствами и дополнительных технических средств (ДТС) (средства связи, системы и средства кондиционирования, сигнализации, электроосвещения, радиовещания, часификации т.п.), находящихся в помещении, где расположено оборудование

ИТС, и в смежных помещениях. Указанные условия размещения и минимально допустимые расстояния берутся из эксплуатационной документации, сопровождающей сертифицированы ОТС.

В случае отсутствия для ОТС, используемых в составе КСЗИ, сертификатов соответствия требованиям по технической защите информации, минимально допустимые расстояния и другие условия размещения этих средств должны быть определены по результатам их специальных исследований на этапе проведения пусконаладочных работ.

В состав рабочей документации на КСЗ должны входить описания процедур установки и запуска комплекса, наладки всех механизмов разграничения доступа пользователей к информации и аппаратных ресурсов ИТС, контроля за действиями пользователей, формирования и актуализации баз данных защиты, а также контроля целостности программного обеспечения баз данных защиты.

Документация рабочего проекта должна содержать исходные данные для внесения их в базы данных защиты.

Эксплуатационная документация включает описание порядка функционирования КСЗИ и руководства (инструкции) по обеспечению этого порядка обслуживающим персоналом и пользователями, порядка сопровождения КСЗИ протяжении жизненного цикла ИТС.

Введение КСЗИ в действие и оценка защищенности информации в ИТС

Введение КСЗИ в действие и оценка защищенности информации в ИТС проводится по этапам:

- подготовка КСЗИ к введению в действие;
- обучение пользователей;
- комплектование КСЗИ;
- выполнение строительно-монтажных работ;
- пуско-наладочные работы;
- предварительные испытания;
- исследовательская эксплуатация;
- государственная экспертиза.

Подготовка КСЗИ до введения в действие предусматривает:

- проведение работ по подготовке организационной структуры и разработки распорядительных документов, регламентирующих деятельность по обеспечению защиты информации в ИТС;
- создание СЗИ (назначаются ответственные лица за защиту информации), если это не было сделано на предыдущих этапах;
- завершение разработки и утверждение документов, входящих в План защиты (за исключением тех, для разработки которых необходимы результаты следующих этапов работ);
- создание СЗИ и разработка Плана защиты осуществляется в соответствии с НД ТЗИ 1.4-001.

Обучение пользователей

Проводится обучение пользователей ИТС всех категорий (технического обслуживающего персонала, обычных пользователей и пользователей, имеющих полномочия по управлению средствами КСЗИ и др.) в части, их касающейся,

основным положениям документов Плана защиты, которые необходимы им для соблюдения правил политики безопасности информации, эксплуатации средств защиты информации и т.п., проверка их умения пользоваться внедренными технологиями защиты информации и регистрация результатов обучения.

Комплектование КСЗИ

Комплектование КСЗИ обеспечивается получением продукции (средств защиты информации, материалов, оборудования и др.) от поставщиков и соисполнителей работ. Принимается решение о подготовке к проведению оценки на соответствие требованиям НД ТЗИ средств защиты, которые на момент проектирования КСЗИ не имели соответствующих сертификата или экспертного заключения, а также порядке проведения такой оценки при государственной экспертизе КСЗИ.

Строительно-монтажные работы

Работы этого этапа выполняются при переоборудовании существующих или при строительстве новых специализированных сооружений (помещений), предназначенных для размещения технических средств ИТС и персонала, хранилищ материальных носителей информации.

При проведении строительно-монтажных работ учитываются требования технического задания на создание КСЗИ в ИТС.

Строительные работы осуществляются силами организации-владельца ИТС или строительно-монтажными организациями согласно проектной документации на строительство, которая разрабатывается проектной организацией в соответствии с требованиями нормативных документов ДБН А.2.2-2, ДБН 2.2-3-2004.

После завершения строительных работ создается комиссия по приемке работ, в состав которой входят представители организации-заказчика строительных работ, проектной и строительно-монтажной организации. По результатам работы комиссии составляется в произвольной форме акт приемки работ по оценке их соответствия требованиям ТЗИ, который утверждается руководителем организации-заказчика строительства.

Пусконаладочные работы

Целью пусконаладочных работ являются:

- монтаж оборудования и аттестация комплекса технической защиты информации от утечки по техническим каналам;
- установка и налаживание КСЗ;
- проверка работоспособности средств защиты информации в автономном режиме и при их комплексном взаимодействии.

Монтаж основних технических средств (ОТС) ИТС, кабельного оборудования, сетей питания и заземления осуществляется согласно конструкторской документации рабочего проекта.

Если в состав КСЗИ входят ОТС, не имеющих сертификатов соответствия требованиям ТЗИ, определяются минимально допустимые расстояния между этими средствами и по результатам их специальных исследований.

В случае невозможности соблюдения требований по размещению ОТС или наличии оснований для возможного нарушения условий их поставки, оценка

монтажных работ ОТС должна быть подтверждена результатами контрольных инструментальных измерений уровня ПЭМИН.

Специальные исследования и инструментальные измерения уровня ПЭМИН выполняются подразделением ТЗИ организации-владельца ИТС или другими субъектами хозяйствования при условии наличия лицензии или разрешения на осуществление соответствующего вида работ.

По результатам работ составляется акт, где указываются: категории помещений, где расположено оборудование ИТС, пределы контролируемых зон для помещений, перечень ОТС, ДТС и коммуникаций (с указанием наименования, типа, заводского номера), находящихся в этих помещениях, оценка соответствии проведение монтажных работ требованиям эксплуатационных документов на средства и нормативных документов предложения по применению дополнительных мер защиты, внедрение которых необходимо в случае невозможности при выполнении монтажных работ соблюдения отдельных требований по размещению ОТС. Акт утверждается руководителем организации - владельца ИТС.

Осуществляется внедрение дополнительных мер защиты, необходимость внедрения которых зафиксирована в акте, в соответствии с порядком проведения работ этапа и соответствующая корректировка проектной, рабочей и эксплуатационной документации.

Оценка полноты и качества выполнения работ по ТЗИ в помещениях проводится путем аттестации внедренного комплекса технической защиты информации от утечки по техническим каналам, по результатам которой предоставляется документ установленного образца - «Акт аттестации комплекса технической защиты информации». Порядок осуществления аттестации, содержание и форма «Акта ...» определяется НД ТЗИ 2.1-001.

Далее осуществляется согласно документации рабочего проекта инсталляция, инициализация и проверка работоспособности КСЗ. Инсталляция и инициализация КСЗ, который имеет экспертное заключение о его соответствии требованиям НД ТЗИ, осуществляется в порядке, определенном в эксплуатационной документации на этот комплекс.

При инсталяции должны быть задействованы все механизмы разграничения доступа пользователей к информации и аппаратных ресурсов ИТС, контроля за действиями пользователей, а также контроля целостности программного обеспечения и базы данных защиты КСЗ.

В базу данных защиты вносятся сведения о пользователях ИТС, устанавливаются их полномочия по доступу к защищаемым объектам компьютерных систем (КС), их создания, модификации, архивирования, уничтожения, экспорта/импорта из системы и другие данные.

Предварительные испытания

Целью предварительных испытаний является проверка работоспособности КСЗИ и определения возможности принятия ее в опытную эксплуатацию.

Во время испытаний проверяются работоспособность КСЗИ и соответствие ее требованиям ТЗ.

Предварительные испытания проводятся согласно программе и методикам испытаний. Программу и методики испытаний готовит разработчик КСЗИ, а согласовывает заказчик ИТС.

Предварительные испытания организует заказчик ИТС, а проводит разработчик КСЗИ совместно с заказчиком. Для проведения предварительных испытаний заказчиком ИТС создается комиссия. Председателем комиссии назначается представитель заказчика.

Результаты предварительных испытаний оформляются «Протоколом испытаний», где содержится вывод о возможности принятия КСЗИ в опытную эксплуатацию, а также перечень выявленных недостатков, необходимых мер по их устранению, и рекомендуемые сроки выполнения этих работ.

После устранения недостатков в случае их наличия и корректировки проектной, рабочей и эксплуатационной документации КСЗИ оформляется акт о приемке КСЗИ в опытную эксплуатацию.

Опытная эксплуатация

Во время опытной эксплуатации КСЗИ:

- отрабатываются технологии обработки информации, обращения машинных носителей информации, управление средствами защиты, разграничение доступа пользователей к ресурсам ИТС и автоматизированного контроля за действиями пользователей;
- сотрудники СЗИ и пользователи ИТС приобретают практические навыки по использованию технических и программно-аппаратных средств защиты информации, усваивают требования организационных и распорядительных документов по вопросам разграничения доступа к техническим средствам и информационным ресурсам;
- осуществляется (при необходимости) доработка программного обеспечения, дополнительное настройки и конфигурирования КСЗ;
- осуществляется (при необходимости) корректировка рабочей и эксплуатационной документации.

По результатам работ в произвольной форме составляется акт о завершении опытной эксплуатации, содержащий заключение о возможности (невозможности) представления КСЗИ на государственную экспертизу.

Государственная экспертиза КСЗИ

Государственная экспертиза КСЗИ является отдельным этапом приемочных испытаний ИТС.

Государственная экспертиза проводится с целью определения соответствия КСЗИ техническому заданию, требованиям НД по защите информации и определение возможности введения КСЗИ в составе ИТС в эксплуатацию.

Государственная экспертиза КСЗИ в ИТС проводится согласно Положению о государственной экспертизе в сфере технической защиты информации.

Обнаруженные при государственной экспертизы недостатки устраняются до ее завершения, порядок устранения такой же, как и для предыдущих испытаний. Если в силу каких-то причин устранить недостатки в ходе экспертизы невозможно, это оформляется актом, в который вносится перечень необходимых

доработок и рекомендации по их выполнению. После завершения предусмотренных актом работ проводится повторная экспертиза.

Для интегрированных ИТС может проводиться государственная экспертиза каждой составной части (модуля) КСЗИ отдельно.

Государственная экспертиза КСЗИ интегрированной ИТС состоит в проверке взаимодействия (администрирование, обмена данными базы данных защиты и т.д.) уже оцененных модулей.

Документы, содержащие результаты работ каждого из этапов (протоколы, акты, аттестаты соответствия) для КСЗИ ИТС в целом, оформляются с учетом соответствующих документов на составные части КСЗИ.

Если интегрированная КСЗИ имеет в своем составе типовые модули, которые создавались по единому ТЗ, то экспертиза таких модулей КСЗИ выполняется в два этапа: на первом проводится в полном объеме экспертиза одного выбранного типового модуля, а на втором - осуществляется проверка соответствия условий эксплуатации типичным на каждом конкретном объекте для всех модулей КСЗИ этого типа.

Введение в состав действующей КСЗИ нового (оцененного) модуля осуществляется без проведения повторной экспертизы всей КСЗИ. Проводится оценивание взаимодействия нового модуля с составными частями КСЗИ, которые уже находятся в эксплуатации.

Допускается начинать и проводить государственную экспертизу КСЗИ параллельно с работами этапов проектирования.

Приемочные испытания ИТС проводятся при функционирующей в ее составе КСЗИ.

Сопровождение КСЗИ

Сопровождение КСЗИ заключается в выполнении работы по организационному обеспечению функционирования КСЗИ и управления средствами защиты информации в соответствии с Планом защиты и эксплуатационной документации на компоненты КСЗИ, гарантийному и послегарантийному техническому обслуживанию средств защиты информации.

2.4 Сертификация, государственный контроль, экспертиза и оценка технических средств защиты информации

Приказом Администрации Государственной службы специальной связи и защиты информации Украины совместно с Государственным комитетом Украины по вопросам технического регулирования и потребительской политики №75/91 от 25.04.2007 г. были утверждены Правила проведения работ по сертификации средств защиты информации. Этот документ устанавливает правила проведения работ по сертификации средств защиты информации в Украинской государственной системе сертификации продукции – УкрСЕРПО (далее - Система).

Общее руководство сертификационной деятельностью в сфере защиты информации, организация и координация работ по сертификации осуществляются национальным органом по сертификации - Государственным комитетом Украины по вопросам технического регулирования и потребительской политики (далее - Госпотребстандарт Украины) и Государственной службой специальной связи и защиты информации Украины (далее - Госспецсвязи).

Сертификацию осуществляют исключительно органы сертификации (ОС), которые предназначены и / или уполномоченные в установленном порядке для выполнения работ по сертификации в Системе и имеют соответствующую область аккредитации.

Сертификационные испытания проводят исключительно исполнительные лаборатории (ИЛ), аккредитованные в установленном порядке на независимость и/или техническую компетентность в соответствии с требованиями ДСТУ 3412-96 или ДСТУ ISO / IEC 17025-2001.

Объектом сертификации в системе УкрСЕПРО являются средства защиты информации.

Сертификация проводится на соответствие требованиям нормативных документов, утвержденных и зарегистрированных в установленном порядке.

Порядок проведения работ по сертификации средств защиты информации в общем случае предусматривает:

- подачу заявки на сертификацию;
- рассмотрение и принятие решения по заявке с указанием схемы (модели) сертификации;
- обследования или аттестацию производства средств защиты информации, сертифицируемых, или сертификацию (оценку) системы качества, если это предусмотрено схемой сертификации;
- отбор образцов средств защиты информации для испытаний;
- идентификацию средств защиты информации;
- прием ИЛ образцов средств защиты информации;
- испытания образцов средств защиты информации;
- анализ полученных результатов испытаний и принятие решения о возможности выдачи сертификата соответствия;
- выдачу сертификата соответствия, заключение лицензионного соглашения и занесение сертифицированных средств защиты информации в Реестр Системы;
- технический надзор за сертифицированными средствами защиты информации при их производства;
- информирование о результатах работ по сертификации средств защиты информации.

Проведение работ по сертификации средств защиты информации.

Подача заявки на сертификацию

Заявителем работ по сертификации средств защиты информации могут быть:

- производитель средств защиты информации;
- поставщик средств защиты информации;

- заказчик (покупатель), которым может быть орган государственной власти или местного самоуправления, предприятие, осуществляющее хозяйственную деятельность, в частности предпринимательскую, в сфере защиты информации.

Для проведения сертификации средств защиты информации в Системе заявитель подает в ОС заявку на проведение сертификации продукции в Системе УкрСЕПРО (далее - заявка)

К заявке прилагаются:

- копия нормативного документа производителя на продукцию (при наличии);
- техническое описание;
- комплект эксплуатационной документации;
- заверенная копия контракта (договора) или другой документ, подтверждающий происхождение средств защиты информации (при наличии).

Технические условия на средства защиты информации должны быть согласованы с Администрацией Госспецсвязи соответствии с постановлением Кабинета Министров Украины от 13 марта 2002 года N 281 «О некоторых вопросах защиты информации, охрана которой обеспечивается государством».

Заявителем дополнительно могут быть переданы в ОС сертификаты, протоколы испытаний, выданные другими ОС или ИЛ (в том числе иностранными), другая документация, позволяющая уточнить особенности средств защиты информации и ускорить процедуру сертификации.

Рассмотрение и принятие решения по заявке с указанием схемы (модели) сертификации

ОС при рассмотрении заявки выполняет следующие процедуры:

- регистрирует заявку в журнале учета и заводит отдельное дело о сертификации средств защиты информации, в которой в дальнейшем хранятся все переписки и документация по этому заявителя;
- проверяет правильность заполнения реквизитов заявки;
- проводит анализ предоставленной документации;
- определяет необходимость разработки программы и методики испытаний отдельных средств защиты информации, которые согласуются с Госспецсвязи;
- определяет схему сертификации по поданной заявке;
- определяет с учетом пожелания заявителя аккредитованные в Системе ИЛ, которые будут проводить испытания образцов;
- определяет количество образцов для испытаний, правила их отбора;
- согласовывает с заявителем сроки проведения работ по сертификации и их стоимость;
- готовит документы по установленной форме для заключения договора с заявителем на проведение работ по сертификации в соответствии с ДСТУ 3410;
- готовит решение по заявке на проведение сертификации продукции в Системе УкрСЕПРО (далее - решение).

По результатам рассмотрения заявки ОС не позднее одного месяца со дня его регистрации направляет заявителю свое решение, в котором указываются основные условия сертификации. В случае положительного решения по заявке

ОС одновременно направляет заявителю проект договора на проведение работ по сертификации.

Копия решения по заявке направляется в:

- органа по сертификации систем качества (в случае необходимости);
- ИЛ (или нескольким ИЛ), которая будет проводить испытания;
- ОС или государственному центру стандартизации, метрологии и сертификации по месту расположения заявителя, которая будет осуществлять технический надзор (если это предусмотрено схемой сертификации).

Если для принятия решения по заявке необходимы дополнительные сведения о средствах защиты информации или его производителя, то ОС по согласованию с заявителем может установить другой срок рассмотрения заявки.

Если по результатам рассмотрения заявки и предоставленной документации окажется невозможным проведение последующих работ по сертификации, то не позднее одной недели заявителю направляется обоснованное решение и заявка аннулируется.

Заявка аннулируется также, если в течение месяца после отправки заявителю органом по сертификации проекта договора на проведение работ по сертификации (или испытательной лабораторией проекта договора на проведение сертификационных испытаний) указанный договор заявителем не был заключен.

Определение схемы (модели) сертификации средств защиты информации

Схема (модель) сертификации определяется ОС при рассмотрении заявки с учетом особенностей производства, испытаний, поставки и использования конкретного средства защиты информации.

При сертификации средств защиты информации используются схемы (модели) сертификации средств защиты информации в Системе. Если ОС избрана схема по выдаче сертификатов соответствия на серийную продукцию сроком на один год, он дополнительно к заявке может запросить информацию и документы согласно перечню дополнительной информации и документации заявки на сертификацию по выдаче сертификатов соответствия на серийное производство средств защиты информации со сроком действия один год.

Обследование производства

Обследование производства проводится с целью установления соответствия фактического состояния производства требованиям нормативной, конструкторской и технологической документации, подтверждения возможности предприятия изготавливать продукцию в соответствии с требованиями нормативных документов, действующих в Украине, выдачи рекомендаций о периодичности и форм проведения технического надзора за производством сертифицированных средств защиты информации.

Порядок обследования производства устанавливается ОС с учетом требований ДСТУ 3957 и особенностей производства конкретных средств защиты информации. Программа обследования производства соглашается с Администрацией Госспецсвязи.

Аттестация производства

Аттестация производства проводится с целью оценки технических возможностей предприятия-производителя по обеспечению стабильного качества средств защиты информации.

Аттестация производства проводится по инициативе заявителя или по решению ОС и осуществляется ОС. Порядок выполнения работ по аттестации производства устанавливается ОС с учетом особенностей производства, конкретных средств защиты информации и требований ДСТУ 3414.

Сертификация системы качества

Сертификация (оценка) системы качества проводится органами, аккредитованными в Системе на право проведения этих работ. Порядок проведения работ определено ДСТУ 3419.

Сертификация (оценка) системы качества выполняется по инициативе заявителя или по решению ОС, если это предусмотрено схемой сертификации.

Отбор образцов средств защиты информации для испытаний

Отбор образцов для испытаний проводится ОС или по его письменному поручению уполномоченным представителем.

Образцы отбираются из изделий, прошедших приемочный контроль производителя. Количество образцов для испытаний должно соответствовать количеству, указанному в решении по заявке. Отбор образцов проводится в присутствии представителя заявителя и оформляется актом отбора образцов в трех экземплярах. Один экземпляр остается у заявителя, второй - направляется в ОС для хранения, третий - к ИЛ, указанной в решении по заявке.

Образцы отбираются для испытаний, должны быть полностью укомплектованы, опломбированы (опечатаны) и упакованы.

Идентификация средств защиты информации

Идентификация средств защиты информации проводится ОС или по его поручению аккредитованной ИЛ. Если ИЛ аккредитована только на техническую компетентность, то идентификация проводится при участии уполномоченного представителя ОС. В обоих случаях идентификация проводится в присутствии заявителя.

Идентификация включает в себя сверку состава представленного для испытаний образца и его технического состояния с содержанием нормативных документов на эту продукцию.

Образцы, которые не прошли идентификацию, на испытания с целью сертификации не принимаются.

По результатам идентификации составляется акт идентификации.

Прием образцов средств защиты информации испытательной лабораторией

Отобранные и идентифицированные образцы средств защиты информации для испытаний с целью сертификации принимает ответственное лицо ИЛ, специально уполномоченное приказом руководителя ИЛ, исключительно при условии, что эти образцы переданы в лабораторию в опломбированном или опечатанном виде, а также при наличии акта отбора образцов и акта идентификации.

Доставку отобранных образцов к ИЛ и возвращение их после испытаний заявитель осуществляет за свой счет.

В случае, если продукция крупногабаритной или нетранспортабельной или требует монтажа на месте, или использование уникального испытательного оборудования и т.д., допускается сертификационные испытания проводить на предприятии производителя или заказчика с использованием его оборудования и средств измерительной техники, которые соответствуют установленным требованиям. Испытания должны проводить специалисты аккредитованной ИЛ.

Испытания образцов средств защиты информации с целью сертификации

Сертификационные испытания образцов средств защиты информации проводятся ИЛ, которые определены в решении ОС по заявке.

Самостоятельное принятие ИЛ решения о проведении сертификационных испытаний образцов не допускается.

Образцы средств защиты информации испытываются на соответствие требованиям нормативных документов, указанных в решении по заявке.

Программа и методика испытаний отдельных средств защиты информации, определяемых ОС, согласно ДСТУ 3412 разрабатываются ИЛ и согласуются с ОС и Администрацией Госспецсвязи.

При сертификации партии средств защиты информации незначительного количества (до 5 изделий) ОС может принять решение не включать в программу испытаний виды испытаний, которые могут привести к разрушению или физического повреждения образцов продукции.

По результатам испытаний ИЛ представляет протокол испытаний продукции в ОС, копию протокола - заявителю, если это предусмотрено договором на проведение работ по сертификации. Протокол испытаний должен быть подписан исполнителями работ и утвержден руководителем ИЛ. Если испытания проводились в ИЛ, аккредитованной только на техническую компетентность, то протокол испытаний подписывается представителем ОС, под контролем которого проводились эти испытания, и утверждается руководителем ОС.

Протокол испытаний должен четко, полностью и недвусмысленно отражать результаты испытаний и другую информацию, касающуюся проведенных испытаний. Количественные результаты должны подаваться с указанием показателей точности и (или) достоверности.

В случае получения отрицательных результатов хотя бы по одному из показателей, испытания с целью сертификации прекращаются. Об отрицательных результатах испытаний ИЛ в срок не позднее двух недель уведомляет заявителя и ОС, который принимает решение о прекращении или продолжении работ по сертификации.

Повторные испытания, в случае их прекращения, могут быть проведены только после представления заявителем новой заявки и предоставления ОС убедительных доказательств проведения производителем корректирующих мероприятий по устранению причин, вызвавших несоответствие установленным требованиям.

ИЛ обеспечивает условия для хранения образцов в течение всего срока испытаний и возвращение их заявителю.

Образцы, которые прошли испытания с целью сертификации, в том числе методом неразрушающего контроля, остаются собственностью заявителя.

ОС, если считает необходимым, оставляет с согласия заявителя в себя или в ИЛ или передает на ответственное хранение заявителю опломбированы образцы - «образцы-свидетели». Место и срок хранения «образцов-свидетелей» оговаривается в договоре.

Анализ полученных результатов испытаний и принятие решения о возможности выдачи сертификата соответствия

При анализе результатов испытаний оценивается их полнота, объективность, достоверность, показатели точности и другие характеристики.

По положительным результатам рассмотрения протокола испытаний и других работ, предусмотренных в решении по заявке, ОС принимает решение о выдаче сертификата соответствия.

Выдача сертификата соответствия и занесение сертифицированных средств защиты информации в Реестр Системы

Сертификат соответствия выдается ОС на единичное изделие, партию с указанием ее количества или средства защиты информации, которые выпускаются предприятием серийно в течение срока, установленного лицензионным соглашением, с правом маркировки знаком соответствия каждой единицы выпущенной продукции.

Срок действия сертификата соответствия определяется ОС с учетом срока действия нормативных документов на средства защиты информации, схемы сертификации, гарантийного срока эксплуатации продукции, но не более сроков, указанных в схеме (модели) сертификации средств защиты информации в Системе УкрСЕПРО или определенных действующим законодательством Украины.

Правила и порядок регистрации сертификатов соответствия на средства защиты информации в Системе определены ДСТУ 3415.

Формы сертификатов соответствия установлены ДСТУ 3498.

Сертификаты соответствия подписываются Председателем (заместителем Председателя) Госспецсвязи и руководителем ОС.

Сертификат соответствия выдается заявителю. При выдаче сертификата соответствия производителю (поставщику) средств защиты информации, которые изготавливаются серийно, ОС заключает с ним лицензионное соглашение по ДСТУ 3413. Копии сертификата соответствия ОС направляет в Реестр Системы и Госспецсвязи.

В случае внесения изменений в конструкцию (состав) средств защиты информации или технологии их изготовления, которые могут повлиять на показатели, подтвержденные во время сертификации, заявитель обязан не позднее, чем за три месяца предупредить об этом ОС, с которым заключено лицензионное соглашение. ОС принимает решение о необходимости проведения новых испытаний или оценки состояния производства продукции.

Если испытания средств защиты информации по отдельным показателям проводились несколькими аккредитованными или признанными ИЛ, то сертификат соответствия выдается при наличии всех необходимых протоколов испытаний с положительными результатами испытаний. В этом случае в сертификате соответствия приводятся ссылки на все протоколы испытаний с указанием ИЛ, проводившие испытания.

Технический надзор за сертифицированными средствами защиты информации при их производстве

Технический надзор за стабильностью показателей, которые подтверждены сертификатом соответствия, при производстве средств защиты информации осуществляет ОС, выдавший сертификат. По предложению ОС надзор может проводиться органами по сертификации систем качества или государственными центрами стандартизации, метрологии и сертификации.

Объем, порядок и периодичность надзора устанавливаются ОС при проведении сертификации и регламентируются программой технического надзора, которая разрабатывается ОС, согласуется с Администрацией Госспецсвязи и утверждается руководителем ОС.

По результатам надзора ОС может приостановить или отменить действие лицензионного соглашения или сертификата соответствия в случае:

- нарушение требований по технологии изготовления, правил приемки, методов контроля и испытаний, обозначения изделий, согласованных с ОС при проведении сертификации;

- изменения нормативных документов на средства защиты информации или методы их испытаний без предварительного согласования с ОС;

- изменения конструкции (состава), комплектности или технологии изготовления средств защиты информации без предварительного согласования с ОС.

Решение о приостановлении действия лицензионного соглашения и (или) сертификата соответствия принимается в случае, если принятием корректирующих мероприятий, согласованных с ОС, предприятие может устранить обнаруженные причины несоответствия и без проведения повторных испытаний ИЛ подтвердить соответствие средств защиты информации требованиям нормативных документов. В противном случае лицензионное соглашение или сертификат отменяются.

Информация о приостановлении или отмене действия сертификата соответствия в недельный срок в письменной форме направляется ОС до сведения заявителя, национального органа по сертификации и Администрации Госспецсвязи.

Действие сертификата соответствия прекращается с момента исключения его из Реестра Системы в соответствии с ДСТУ 3415.

В случае приостановления действия сертификата соответствия осуществляются такие корректирующие мероприятия:

Орган по сертификации:

- информирует о приостановлении или возобновлении действия сертификата соответствия национальный орган по сертификации и Администрацию Госспецсвязи;

- устанавливает срок выполнения корректирующих мероприятий;

- контролирует выполнение заявителем корректирующих мероприятий.

Заявитель:

- определяет объем изготовленных несоответствующих средств защиты информации и новую маркировку для различения средств защиты информации, произведенных до и после проведения корректирующих мероприятий;

- сообщает потребителя об опасности (или нежелательности) эксплуатации средств защиты информации и порядок устранения выявленных несоответствий или обмена средств защиты информации;

устраняет несоответствия в средствах защиты информации, находящихся в эксплуатации, или обеспечивает их возврат и доработку, заменяет средства защиты информации у потребителя, если устранение выявленных несоответствий невозможно или нецелесообразно;

осуществляет меры по устранению причин несоответствий средств защиты информации.

Сертификация импортируемых технических средств защиты информации

Сертификация единичных образцов и партии средств защиты информации, которые импортируются, проводится аналогично сертификации образцов средств защиты отечественного производства. Возможно также и признание результатов сертификации, подтверждающих соответствие импортируемых средств защиты информации требованиям действующих в Украине нормативных документов и выданных на них за рубежом.

Признание результатов сертификации средств защиты информации, импортируемых касается:

- сертификата (знака) соответствия;

- результатов испытания ИЛ.

Решение о признании результатов сертификации принимает ОС на основании подтверждения соответствия продукции требованиям нормативных документов, действующих в Украине, а также аналогичным требованиям нормативных документов других стран.

Сертификаты соответствия и протоколы испытаний, выданные уполномоченными органами других стран, подлежат признанию в Системе при условии соблюдения совокупности таких правил:

- национальным органом по сертификации заключено двустороннее соглашение о взаимном признании результатов работ по сертификации с национальным органом по сертификации той страны, из которой происходят средства защиты информации, которые ввозятся в Украину;

- средства защиты информации, которые ввозятся в Украину, могут быть идентифицированы по сопроводительной документации (маркировка, этикетка) как, изготовленные по межгосударственным или другими нормативными документами, которые действуют в Украине;

- указанная в иностранном сертификате соответствия номенклатура требований к средствам защиты информации и нормы этих требований полностью отвечают номенклатуре требований к этой продукции и нормам, действующим в Украине. При условии выполнения совокупности указанных правил, ОС выдает на иностранный сертификат свидетельство о его признании, которое подписывает Председатель (заместитель Председателя) Госспецсвязи и руководитель ОС.

В случае невыполнения хотя бы одного из условий правил, сертификация средств защиты информации иностранного производства осуществляется аналогично сертификации образцов средств защиты отечественного производства.

Документом о признании иностранных сертификатов соответствия является свидетельство о признании (в случае полного признания) или сертификат соответствия (в случае частичного признания), выданные в Системе.

Процедура признания результатов сертификации средств защиты информации, импортируемых должен соответствовать ДСТУ 3417.

Положение о государственном контроле за состоянием технической защиты информации утверждено приказом Администрации Государственной службы специальной связи и защиты информации Украины №87 от 16.05.2007 г.

Данное Положение определяет порядок организации и осуществления государственного контроля за состоянием технической защиты информации, которая принадлежит к государственным информационным ресурсам, или информации с ограниченным доступом, требование относительно защиты которой установлена законом.

Государственный контроль за состоянием технической защиты информации (далее - ТЗИ) осуществляется Государственной службой специальной связи и защиты информации Украины (далее - Госспецсвязи) в соответствии с Законами Украины «О Государственной службе специальной связи и защиты информации Украины», «О защите информации в информационно-телекоммуникационных системах» и Положения об Администрации Государственной службы специальной связи и защиты информации, утвержденного постановлением Кабинета Министров Украины от 24.06.2006 г. №868.

Действие Положения распространяется на все субъекты системы технической защиты информации.

Государственный контроль за состоянием технической защиты информации, которая принадлежит к государственным информационным ресурсам, или информации с ограниченным доступом, требование относительно защиты которой установлена законом, осуществляется в органах государственной власти, органах местного самоуправления, образованных в соответствии с законодательством воинских формированиях, на предприятиях, в учреждениях и организациях независимо от формы собственности, в том числе в зарубежных дипломатических учреждениях Украины, а также в местах постоянного и временного пребывания высших должностных лиц государства (далее - органы, в отношении которых осуществляется ТЗИ).

Государственный контроль за состоянием ТЗИ заключается в проверке выполнения требований нормативно-правовых актов и нормативных документов по ТЗИ и осуществляется с целью определения состояния ТЗИ в органах, в отношении которых осуществляется ТЗИ, выявления нарушений по ТЗИ и их устранения.

Государственный контроль за состоянием ТЗИ осуществляется Госспецсвязи путем организации и проведения контрольно-инспекторской работы по вопросам ТЗИ относительно органов, в отношении которых осуществляется ТЗИ.

Контрольно-инспекторская работа по вопросам ТЗИ включает планирование, проведение инспекционных проверок состояния ТЗИ в органах, в отношении которых осуществляется ТЗИ (далее - проверка), анализ их результатов и предоставления рекомендаций по совершенствованию состояния ТЗИ в указанных органах.

По результатам контрольно-инспекторской работы осуществляются анализ и обобщение состояния ТЗИ в государстве.

Аналитические материалы о состоянии ТЗИ в государстве подаются Президенту Украины, Председателю Верховной Рады Украины и Премьер-министру Украины.

Проверки состояния ТЗИ делятся на комплексные, целевые (тематические) и контрольные. Указанные проверки могут быть плановыми и внеплановыми.

При комплексной проверке определяется соответствие комплекса ТЗИ (комплексной системы защиты информации) и мер противодействия техническим разведкам требованиям нормативно-правовых актов и нормативных документов системы ТЗИ.

При целевой (тематической) проверке проверяются отдельные составляющие комплекса ТЗИ (комплексной системы защиты информации) и мер противодействия техническим разведкам на соответствие внедренных мероприятий требованиям нормативно-правовых актов и нормативных документов системы ТЗИ.

При контрольной проверке проверяется полнота и достаточность принятых мер по устранению недостатков, выявленных в ходе проведения предварительной комплексной или целевой проверки. Контрольные проверки проводятся при необходимости, как правило, после получения уведомления об устранении недостатков.

Плановые проверки осуществляются в соответствии с годовым планом контрольно-инспекторской работы по ТЗИ, утвержденным Председателем Госспецсвязи. Выдержки из плана контрольно-инспекторской работы направляются в центральные органы исполнительной власти и в случае необходимости к предприятиям, учреждениям и организациям.

Внеплановые проверки осуществляются при наличии сведений о нарушениях требований нормативно-правовых актов по вопросам ТЗИ или с целью определения полноты и достаточности мероприятий по ТЗИ, принятых органами, относительно которых осуществляется ТЗИ. Указанные проверки могут проводиться с предупреждением или без предупреждения.

Руководству органов, в отношении которых осуществляется ТЗИ, сообщается о проведении проверки не менее чем за десять дней до ее начала (за исключением проведения внеплановой проверки).

Проверки состояния ТЗИ осуществляются должностными лицами структурного подразделения Администрации Госспецсвязи по вопросам государственного контроля за состоянием криптографической и технической защиты информации и региональных органов Госспецсвязи. К проверкам могут привлекаться специалисты других подразделений Госспецсвязи, а также органов государственной власти, органов местного самоуправления, воинских формирований, предприятий, учреждений и организаций по согласованию с их руководителями.

Основанием для допуска должностных лиц Госспецсвязи к проверке состояния ТЗИ является наличие предписания на право проведения проверки за подписью руководства Администрации Госспецсвязи или начальника регионального органа Госспецсвязи.

Должностные лица Госспецсвязи, включенные в предписания на право проведения проверки, являются уполномоченными лицами для составления протоколов об административных правонарушениях.

Должностные лица Госспецсвязи, осуществляющих проверки состояния ТЗИ, имеют право:

- доступа на объекты информационной деятельности органов, в отношении которых осуществляется ТЗИ, для осуществления государственного контроля за состоянием ТЗИ, а также к другим помещениям (на территорию, в сооружения и т.п.) для изучения вопросов, непосредственно связанных с проверкой;
- знакомиться с любыми документами, необходимыми для проверки;
- бесплатно получать копии необходимых документов, письменные объяснения должностных лиц (справки и т.п.) по вопросам, возникающим в ходе проверки;
- предоставлять по результатам проверок рекомендации по приведению состояния ТЗИ в соответствие с требованиями нормативно-правовых актов и осуществлять контроль за ходом их выполнения;
- ставить в установленном порядке вопрос о приостановлении действия или отмены специальных разрешений на осуществление деятельности, связанной с государственной тайной, в случае выявления нарушений по технической защите секретной информации;
- составлять протоколы об административных правонарушениях и предоставлять в суд на рассмотрение дела об административных правонарушениях.

При установлении фактов совершения нарушений, предусмотренных Кодексом Украины об административных правонарушениях, должностными лицами Госспецсвязи, в пределах полномочий, определенных статьей 255 Кодекса Украины об административных правонарушениях, составляется протокол об административном правонарушении.

Для проверки состояния ТЗИ должностные лица Госспецсвязи должны предъявить руководителю или уполномоченному представителю органа, по

которому осуществляется ТЗИ, предписание на право проведения проверки и служебные удостоверения.

При проведении проверки состояния ТЗИ контролируется полнота и достаточность внедренных на объектах информационной деятельности и объектах противодействия мер по ТЗИ, их соответствие требованиям нормативно-правовых актов, выполнение рекомендаций по устранению нарушений по ТЗИ.

По результатам проверок должностными лицами Госспецсвязи, которые их осуществляли, составляются акты проверок состояния ТЗИ.

Акт комплексной проверки состояния ТЗИ составляется по установленной форме. Акты контрольных и целевых (тематических) проверок составляются в произвольной форме.

Акт проверки состояния ТЗИ готовится в двух экземплярах. Первый экземпляр акта проверки направляется субъекту системы ТЗИ, который проверялся, второй - структурному подразделению Администрации Госспецсвязи по вопросам государственного контроля за состоянием криптографической и технической защиты информации.

В случае проведения проверки региональным органом Госспецсвязи готовится третий экземпляр, который направляется в орган Госспецсвязи, должностные лица которого осуществляли проверку.

Все экземпляры акта подписываются должностными лицами Госспецсвязи, которым проводилась проверка, и утверждаются руководителем Администрации Госспецсвязи или начальником регионального органа Госспецсвязи, который подписал предписание на проведение проверки.

Ознакомление руководителя органа, по которому осуществляется ТЗИ, с актом осуществляется за его подписью.

В случае отказа руководителя органа, по которому осуществляется ТЗИ, засвидетельствовать факт ознакомления с актом проверки своей подписью, должностными лицами Госспецсвязи, осуществлявших проверку, делается в акте соответствующая запись.

Нарушения требований по ТЗИ делятся на три категории, которые определяют возможность реализации угроз безопасности информации:

- первая категория - невыполнение требований нормативно-правовых актов и нормативных документов по ТЗИ, вследствие чего создается реальная угроза нарушения конфиденциальности, в частности за счет утечки (пропитки) техническими каналами, и (или) целостности и доступности информации;

- вторая категория - невыполнение требований нормативно-правовых актов и нормативных документов по ТЗИ, вследствие чего создаются предпосылки к нарушению конфиденциальности, в частности за счет утечки (пропитки) техническими каналами, и (или) целостности и доступности информации;

- третья категория - невыполнение других требований по ТЗИ.

Признаки нарушений первой категории:

- установления факта циркуляции информации с ограниченным доступом на объектах информационной деятельности, в информационных или информационно-телекоммуникационных системах в условиях подтверждения

инструментально-расчетными методами наличии технического канала распространения информации с ограниченным доступом;

- установления факта обработки информации с ограниченным доступом в информационных, телекоммуникационных или информационно-телекоммуникационных системах, имеющих выход незащищенными каналами связи за пределы контролируемой зоны, в условиях отсутствия аттестата соответствия на комплексную систему защиты информации;

- установления факта обработки информации с ограниченным доступом в информационных или информационно-телекоммуникационных системах, не имеющих выхода за пределы контролируемой зоны, в условиях доступа к ее информационным ресурсам пользователей, которые имеют разные полномочия (права доступа к информации), и отсутствия аттестата соответствия на комплексную систему защиты информации;

- установления факта обработки открытой информации, которая принадлежит к государственным информационным ресурсам, требование относительно защиты которой установлена законом, в информационно-телекоммуникационных системах, имеющих подключение к телекоммуникационным сетям (в том числе телекоммуникационных сетей общего пользования), в условиях отсутствия аттестата соответствия на комплексную систему защиты информации;

- установления факта несанкционированного доступа пользователей информационных, телекоммуникационных или информационно-телекоммуникационных систем к информации, которая принадлежит к государственным информационным ресурсам, или информации с ограниченным доступом путем нарушение установленных правил разграничения доступа или преодоления мер защиты.

Признаки нарушений второй категории:

- установления факта циркуляции информации с ограниченным доступом на объектах информационной деятельности, в информационных, телекоммуникационных или информационно-телекоммуникационных системах при отсутствии подтверждения инструментально-расчетными методами соответствия комплекса ТЗИ нормам и требованиям по ТЗИ;

- установления факта обработки информации с ограниченным доступом в информационно-телекоммуникационных системах, имеющих выход за пределы контролируемой зоны защищенными каналами, в условиях отсутствия аттестата соответствия на комплексную систему защиты информации;

- установления факта обработки информации, которая принадлежит к государственным информационным ресурсам, или информации с ограниченным доступом в информационных, телекоммуникационных или информационно-телекоммуникационных системах, не имеющих выхода за пределы контролируемой зоны, в условиях отсутствия аттестата соответствия на комплексную систему защиты информации.

Невыполнение требований нормативно-правовых актов по внедрению организационных мер по ТЗИ, а также других норм и требований в области

защиты информации, которые не приводят к нарушениям первой или второй категории, квалифицируется как нарушение третьей категории.

Заключение проверки является результатом административно-правовой оценки состояния ТЗИ, полноты и достаточности мероприятий по внедрению комплекса технической защиты информации (комплексной системы защиты информации) и мер противодействия техническим разведкам, их соответствия требованиям нормативно-правовых актов по ТЗИ.

Основным критерием соответствия состояния ТЗИ требованиям нормативных документов и нормативно-правовых актов является отсутствие нарушений по ТЗИ.

Выводы проверок состояния ТЗИ и критерии их составления могут быть следующими:

1) Состояние технической защиты информации соответствует требованиям нормативно-правовых актов.

Критерием вывода является отсутствие каких-либо нарушений норм и требований по ТЗИ.

2) Состояние технической защиты информации соответствует требованиям нормативно-правовых актов за исключением выявленных недостатков.

Критерием вывода является наличие хотя бы одного нарушения по ТЗИ третьей категории.

3) Состояние технической защиты информации не в полной мере отвечает требованиям нормативно-правовых актов, что создает предпосылки для нарушения ее конфиденциальности, целостности, доступности и (или) утечки по техническим каналам.

Критерием вывода является наличие хотя бы одного нарушения по ТЗИ второй категории.

4) Состояние технической защиты информации не соответствует требованиям нормативно-правовых актов, что создает реальную угрозу нарушения ее конфиденциальности, целостности, доступности и (или) утечки по техническим каналам.

Критерием вывода является наличие хотя бы одного нарушения по ТЗИ первой категории.

Заключение по результатам контрольной проверки, кроме оценки состояния ТЗИ, должно отражать полноту выполнения рекомендаций (выполнено, не выполнено, выполнено не в полном объеме) по приведению состояния ТЗИ в соответствие с требованиями нормативно-правовых актов и нормативных документов по ТЗИ, указанных в акте предыдущей проверки.

Заключение по результатам целевой (тематической) проверки должно определять оценку состояния ТЗИ по отдельным составляющим комплекса технической защиты информации (комплексной системы защиты информации), которые проверялись.

С целью приведения состояния ТЗИ в соответствие с требованиями нормативно-правовых актов и нормативных документов по ТЗИ должностными лицами Госспецсвязи, которые осуществляли проверку, в акте проверки указываются конкретные рекомендации по устранению выявленных нарушений,

выполнение которых является обязательным для должностных лиц органов, относительно которых осуществляется ТЗИ.

Для выяснения причин, которые привели к нарушениям первой категории, а также привлечение лиц, их совершивших, к ответственности, должностными лицами Госспецсвязи инициируется проведение соответствующих расследований.

В случае выявления нарушений по ТЗИ первой или второй категории должностными лицами Госспецсвязи, осуществлявших проверку, в установленном порядке может ставиться вопрос о прекращении информационной деятельности на соответствующих объектах.

Разрешение на возобновление работ, при выполнении которых были выявлены нарушения норм и требований по ТЗИ первой или второй категории, дает руководитель органа, по которому осуществляется ТЗИ, по согласованию с Госспецсвязи после устранения нарушений.

С целью приведения состояния ТЗИ в соответствие с требованиями нормативно-правовых актов и нормативных документов по ТЗИ, а также выполнения рекомендаций, указанных по результатам проверки, руководителем органа, в отношении которого осуществляется ТЗИ, в месячный срок после получения акта проверки утверждается план устранения недостатков, один экземпляр которого направляется в орган Госспецсвязи, должностными лицами которого была проведена проверка.

Сообщение о выполнении рекомендаций по приведению состояния ТЗИ в соответствие с требованиями нормативно-правовых актов и нормативных документов по ТЗИ направляется руководителю подразделения Госспецсвязи, должностными лицами которого была проведена проверка, в сроки, указанные в акте проверки и плане устранения недостатков.

Руководители органов, в отношении которых осуществляется ТЗИ, имеют право обжаловать результаты проверок в порядке, определенном законодательством Украины.

Должностные лица органов, в отношении которых осуществляется ТЗИ, во время проверки обязаны предоставлять все необходимые для проведения проверки документы и обеспечивать условия для ее проведения.

За препятствование законной деятельности Госспецсвязи при осуществлении государственного контроля за состоянием ТЗИ виновные лица несут ответственность согласно законодательству Украины.

Должностные лица и граждане, виновные в невыполнении норм и требований технической защиты секретной информации, вследствие чего возникает реальная угроза нарушения конфиденциальности, в частности за счет утечки (пропитки) техническими каналами, целостности и доступности этой информации, несут ответственность согласно законодательству Украины.

Руководители органов, в отношении которых осуществляется ТЗИ, обязаны принять неотложные меры по выполнению рекомендаций, изложенных в актах проверок, и несут персональную ответственность за приведение состояния ТЗИ в соответствие с требованиями нормативно-правовых актов системы ТЗИ.

Должностные лица Госспецсвязи за нарушение конституционных прав и свобод человека и гражданина в ходе осуществления государственного контроля за состоянием ТЗИ несут ответственность согласно законодательству Украины.

Положение о государственной экспертизе в сфере технической защиты информации утверждено приказом Администрации Государственной службы специальной связи и защите информации Украины №93 от 16.05.2007 г.

Государственная экспертиза в сфере технической защиты информации (экспертиза) проводится с целью исследования, проверки, анализа и оценки объектов экспертизы для возможного их использования по обеспечению технической защиты информации.

Действие этого Положения распространяется на всех юридических и физических лиц, являющихся субъектами экспертизы.

Субъектами экспертизы являются:

- юридические и физические лица, которые выступают заказчиками экспертизы (далее - Заказчики);
- Администрация Государственной службы специальной связи и защиты информации Украины (далее - Администрация);
- подразделения Государственной службы специальной связи и защиты информации Украины, предприятия, учреждения и организации, которые проводят экспертизу (далее - Организаторы);
- государственные органы, которые проводят экспертизу в сфере своего управления;
- физические лица - исполнители экспертных работ по ТЗИ (далее - Эксперты).

Объектами экспертизы являются:

- комплексные системы защиты информации (далее - КСЗИ), которые являются неотъемлемой составной частью информационной, телекоммуникационной или информационно-телекоммуникационной системы (далее - ИТС);
- технические и программные средства, реализующие функции ТЗИ (далее - средства ТЗИ).

Экспертиза может быть первичной, дополнительной и контрольной.

Первичная экспертиза является основным видом экспертизы и предусматривает выполнение Организатором всех необходимых мероприятий для подготовки и принятия решения относительно объекта экспертизы.

Дополнительная экспертиза проводится в отношении объектов экспертизы, относительно которых открылись новые научные и научно-технические обстоятельства или в связи с окончанием срока действия документов, удостоверяющих результаты экспертизы.

Контрольная экспертиза проводится другим Организатором по инициативе Заказчика при наличии у него обоснованных претензий к выводу первичной или дополнительной экспертизы или по инициативе Администрации для проверки заключения первичной или дополнительной экспертизы.

Для организации и проведения экспертизы Администрация:

- разрабатывает необходимые нормативно-правовые акты и нормативные документы, обеспечивающие проведение экспертизы, информирует Организаторов и Экспертов относительно введения их в действие;

- формирует реестры Организаторов и Экспертов;

- регистрирует заявления на проведение экспертизы, предоставляет Заказчикам и Организаторам консультации относительно порядка и организации проведения экспертизы, оформления документов по результатам проведения экспертизы;

- принимает решение о возможности и целесообразности проведения и организации экспертизы, в частности контрольной;

- в случае экспертизы средства ТЗИ принимает решение о необходимости разработки порядка отбора образцов для проведения испытаний;

- регистрирует, выдает, приостанавливает действие или аннулирует экспертные заключения о возможности использования средств ТЗИ (далее - Экспертные заключения) и аттестаты соответствия КСЗИ требованиям нормативных документов по ТЗИ (далее - Аттестаты);

- осуществляет контроль за проведением Организатором экспертных испытаний и за соблюдением требований эксплуатации объекта экспертизы, которые влияют на защищенность информации.

Заказчик экспертизы имеет право:

- использовать без ограничений выводы, результаты и материалы экспертизы в своей деятельности, если иное не предусмотрено договором на проведение экспертизы;

- заявлять о необходимости проведения контрольной или дополнительной экспертизы;

- принимать по согласованию с Организатором участие в проведении экспертных работ;

- обращаться к Администрации по вопросам проведения Организатором экспертных испытаний.

Заказчик экспертизы обязан:

- способствовать Организатору в проведении всестороннего комплексного исследования объекта экспертизы для формирования экспертной оценки;

- передавать Организатору в установленные договором сроки необходимые материалы, расчеты, данные, дополнительные сведения, касающиеся объекта экспертизы и оказывать необходимое для проведения экспертизы оборудование.

Организатор экспертизы имеет право:

- осуществлять все необходимые меры с целью организации и проведения экспертизы согласно договорным условиям с Заказчиком;

- готовить предложения по внесению (изъятию) специалистов по вопросам ТЗИ в (из) реестр(а) экспертов;

- готовить предложения по разработке и разрабатывать проекты нормативных документов по вопросам проведения экспертизы.

Организатор экспертизы обязан:

- обеспечивать беспристрастное, объективное и своевременное проведение экспертизы;

- осуществлять мероприятия для обеспечения контроля со стороны Администрации за проведением экспертных испытаний;

- рассматривать по поручению Администрации проекты нормативных документов по выполнению экспертных работ и предоставлять содержательные, обоснованные предложения и замечания;

- выполнять требования к конфиденциальности проведения экспертизы.

Эксперт имеет право:

- свободно излагать личное мнение по вопросам экспертизы, а также по результатам выполнения работ;

- требовать от Организатора предоставления достоверных сведений, материалов, инженерно-технического обеспечения, необходимых для выполнения экспертных работ и подготовки заключений;

- вносить предложения по совершенствованию форм и методов проведения экспертизы.

Эксперт обязан:

- объективно, беспристрастно и своевременно выполнять экспертные работы;

- не допускать разглашения информации, содержащейся в материалах и выводах экспертизы;

- предъявлять по требованию Заказчика документы, подтверждающие его опыт и уровень квалификации.

Для проведения экспертизы Заказчик направляет заявление на имя Председателя (заместителя Председателя) Госспецсвязи о проведении экспертизы КСЗИ в ИТС или средства ТЗИ.

С целью рассмотрения заявлений, координации мероприятий и принятия решений о проведении экспертиз в Администрации создается экспертный совет по вопросам государственной экспертизы в сфере технической защиты информации (далее - Экспертный совет), деятельность которой определяется соответствующим положением об этом органе.

По результатам рассмотрения заявления Экспертный совет в месячный срок принимает решение о целесообразности проведения экспертизы и определяет ее Организатора.

В случае наличия у Заказчика обоснованных претензий относительно порядка проведения или результатов экспертизы он может обратиться к Администрации с предложением относительно осуществления контроля за проведением Организатором экспертных испытаний или с заявлением на имя Председателя (заместителя Председателя) Госспецсвязи о проведении контрольной экспертизы.

Порядок подачи и рассмотрения заявления Заказчика о проведении контрольной экспертизы КСЗИ в ИТС или средства ТЗИ осуществляется аналогично.

Основным документом, регламентирующим отношения между Заказчиком и Организатором, является заключенный между ними договор на проведение экспертизы. Порядок финансирования экспертизы определяется в соответствии с законодательством Украины.

Результаты, материалы, выводы экспертизы и созданное или приобретенное за средства Заказчика материально-техническое обеспечение являются его собственностью, если иное не предусмотрено договором между Заказчиком и Организатором.

Срок проведения экспертизы определяется договором и не должен превышать шести месяцев. В случае значительного объема экспертных работ срок проведения экспертизы может быть продлен с согласия Администрации и Заказчика.

Список экспертов, которые привлекаются к выполнению экспертных работ, определяется Организатором.

Заказчик предоставляет Организатору комплект организационно-технической документации на объект экспертизы, необходимый для проведения экспертных испытаний.

Организатор по результатам анализа предоставленных документов и с учетом общих методик оценивания задекларированных характеристик средств ТЗИ и КСЗИ, формирует программу и отдельные методики проведения экспертизы объекта и разрабатывает, при необходимости, порядок отбора образцов средств ТЗИ для проведения испытаний и соответствующее программно-техническое обеспечение.

Программа проведения экспертизы согласовывается с Заказчиком и Департаментом по вопросам защиты информации в информационно-телекоммуникационных системах Администрации, а отдельные методики - с указанным департаментом.

Сроки разработки отдельной методики и необходимых программно-аппаратных средств зависят от характера и сложности объекта экспертизы и определяются в договоре на проведение экспертизы.

При проведении экспертизы каждый Эксперт выполняет экспертные работы только по поручению Организатора в соответствии с определенной отдельной методикой. Результаты работы оформляются в виде протокола выполнения работ за подписью экспертов, которые ее выполняли. Протокол утверждается Организатором. Организатор может рекомендовать Эксперту осуществить изменения протоколов выполненных работ без изменения их содержания (стилистическое редактирование).Согласование результатов отдельных работ между Экспертом и Организатором, а также внесения изменений в протоколы после их оформления или сочетание результатов отдельных работ в одном протоколе не разрешается. В протоколе могут быть зафиксированы особые мнения экспертов относительно результатов выполненных работ.

В случае выявления несоответствия объекта экспертизы требованиям нормативных документов по ТЗИ Организатор может предложить Заказчику выполнить доработку объекта. Срок доработки объекта экспертизы определяется общим протоколом или дополнительным соглашением к договору между Заказчиком и Организатором.

Сведения о всех доработок, а также результаты дополнительных экспертных работ оформляются отдельными протоколами.

Результаты работ, определенных отдельной методикой, обобщаются Организатором в Экспертном заключении. Выводы по каждому пункту отдельной методики, а также особые мнения экспертов, зафиксированные в протоколах, включаются в Экспертного заключения как составные части без внесения в них каких-либо изменений.

По результатам проведенных работ Организатор составляет Экспертное заключение соответствующего содержания о соответствии объекта экспертизы требованиям нормативных документов по ТЗИ, подписывает его и подает в Администрации.

Экспертное заключение на средство ТЗИ рассматривается Экспертным советом и, в случае утверждения результатов экспертизы, регистрируется и выдается Заказчику. На основании положительного решения по экспертизе КСЗИ Заказчику выдается зарегистрирован Аттестат соответствия за подписью Председателя (заместителя Председателя) Госспецсвязи. Экспертные заключения на средства ТЗИ и Аттестаты печатаются на бланках строгого учета, изготавливаемых в установленном законодательством порядке. Администрация имеет право приостановить или аннулировать действие Экспертного заключения или Аттестата.

Администрация предоставляет государственному органу полномочия по организации и проведению первичных или дополнительных экспертиз КСЗИ в ИТС при условии согласования с Администрацией порядка их осуществления. Государственные органы, имеющие разрешение Администрации на проведение работ по ТЗИ для собственных нужд и получившие от Администрации указанные полномочия:

- осуществляют организацию и проведение экспертиз КСЗИ в ИТС в сфере своего управления;
- выдают Аттестат соответствия, который регистрируется Администрацией.

Порядок оценки защищенности государственных информационных ресурсов в информационных, телекоммуникационных и информационно-телекоммуникационных системах утвержден приказом Администрации Государственной Службы специальной связи и защиты информации Украины №112 от 04.07.2008 г. Этот порядок определяет правовые и организационные основы проведения оценки состояния защищенности государственных информационных ресурсов в ИТС в органах государственной власти, органах местного самоуправления, воинских формированиях, на предприятиях, в учреждениях и организациях независимо от форм собственности.

Объектом оценки состояния защищенности является состояние защищенности государственных информационных ресурсов, которые обрабатываются в информационных, телекоммуникационных и информационно-телекоммуникационных системах, независимо от наличия комплексной системы защиты информации.

Оценка состояния защищенности осуществляется с целью выявления существующих угроз государственным информационным ресурсом в ИТС и является составной частью мер защиты информации.

В ИТС, где созданы КСЗИ с подтвержденным соответствием, оценка состояния защищенности проводится с целью выявления угроз государственным информационным ресурсам, возникшим в процессе эксплуатации КСЗИ вследствие несоблюдения требований нормативных актов в области защиты информации в ИТС и не учтенных в КСЗИ.

В случае выявления в ИТС, где созданы КСЗИ с подтвержденным соответствием, дополнительных угроз государственным информационным ресурсам, возникшим за период эксплуатации КСЗИ, информация о такой КСЗИ предоставляется Госспецсвязи согласно Положению о Реестре информационных, телекоммуникационных и информационно-телекоммуникационных систем органов исполнительной власти, а также предприятий, учреждений и организаций, относящихся к сфере их управления, утвержденным постановлением Кабинета Министров Украины от 03.08.2005 N 688.

Оценка состояния защищенности в органах государственной власти, органах местного самоуправления, вооруженных силах, на предприятиях, в учреждениях, организациях независимо от формы собственности осуществляется Госспецсвязью.

По результатам оценки состояния защищенности составляется акт оценки состояния защищенности государственных информационных ресурсов в информационных, телекоммуникационных и информационно-телекоммуникационных системах (Акт), где излагаются результаты работы комиссии и рекомендации по повышению уровня защищенности государственных информационных ресурсов, который утверждается Председателем Госспецсвязи или его заместителем по направлению деятельности согласно распределению функциональных обязанностей.

С целью осуществления оценки состояния защищенности Госспецсвязи:

- создает комиссию по оценке состояния защищенности (далее - комиссия);

- осуществляет планирование проведения оценки состояния защищенности в органах государственной власти, органах местного самоуправления, воинских формированиях, на предприятиях, учреждениях и организациях независимо от форм собственности;

- разрабатывает общую программу и методику оценки состояния защищенности в органах государственной власти, органах местного самоуправления, воинских формированиях, на предприятиях, учреждениях и организациях независимо от форм собственности, а также отдельные программы и методики оценки защищенности зависимости от вида ИТС и режима доступа к информации, которая в них обрабатывается;

- определяет перечень документов, касающихся функционирования ИТС и подлежащих анализу при проведении оценки состояния защищенности;

- определяет и публикует на официальном сайте Госспецсвязи в сети Интернет перечень специализированного программного обеспечения и программно-аппаратных средств, используемых для проведения оценки защищенности;

- органы государственной власти, органы местного самоуправления, воинские формирования, предприятия, учреждения и организации независимо от

форм собственности, в отношении ИТС, на которых осуществляется оценка состояния защищенности государственных информационных ресурсов:

- предоставляют комиссии все необходимые документы, касающиеся функционирования ИТС;

- предоставляют комиссии доступ к ИТС;

- сообщают Госспецсвязи об учете или неучете рекомендаций, указанных в Акте.

Оценка состояния защищенности в органах государственной власти, органах местного самоуправления, воинских формированиях, на предприятиях, учреждениях и организациях независимо от форм собственности, в ИТС, на которых обрабатываются государственные информационные ресурсы, проводится согласно годовому плану, который утверждается приказом Администрации Госспецсвязи, или внепланово.

Плановая оценка состояния защищенности проводится в органах государственной власти, воинских формированиях, на предприятиях, учреждениях и организациях независимо от форм собственности не чаще чем раз в пять лет.

Выдержки из годового плана направляются в указанные в нем органы государственной власти, органы местного самоуправления, воинские формирования, предприятия, учреждения и организация независимо от форм собственности ежегодно до 1 февраля.

Внеплановая оценка состояния защищенности проводится в органах государственной власти, органах местного самоуправления, воинских формированиях, на предприятиях, учреждениях и организациях независимо от форм собственности по их непосредственным обращениям и решению Председателя Госспецсвязи или его заместителя по направлению деятельности согласно распределению функциональных обязанностей.

Госспецсвязи письменно уведомляет органы государственной власти, органы местного самоуправления, воинские формирования, предприятия, учреждения, организации независимо от формы собственности, в ИТС которых планируется осуществить оценку состояния защищенности, не менее чем за десять дней до ее начала.

Основанием для допуска к проведению оценки состояния защищенности является предписание, подписанное Председателем Госспецсвязи или его заместителем по направлению деятельности согласно распределению функциональных обязанностей, в котором указывается состав комиссии.

2.5 Ответственность за нарушение законодательства о защите информации в информационных, телекоммуникационных и информационно-телекоммуникационных системах

Лица, виновные в нарушении порядка и правил защиты обрабатываемой информации в информационных, телекоммуникационных и информационно-

телекоммуникационных системах несут дисциплинарную, административную, уголовную ответственность согласно действующему законодательству Украины.

Так, наиболее распространенным преступлением в сфере использования электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей и сетей электросвязи являются преступления, ответственность за которые предусмотрены статьями 361, 361-1, 361-2, 362, 363, 363-1 Уголовного Кодекса Украины.

Статья 361 Несанкционированное вмешательство в работу электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи

1. Несанкционированное вмешательство в работу электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи, которое привело к утечке, потере, подделке, блокированию информации, искажению процесса обработки информации или к нарушению установленного порядка ее маршрутизации, - наказывается штрафом от шестисот до тысячи необлагаемых минимумов доходов граждан или ограничением свободы на срок от двух до пяти лет, или лишением свободы на срок до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет или без такового и с конфискацией программных и технических средств, с помощью которых было совершено несанкционированное вмешательство, которые являются собственностью виновного лица.

2. Те же действия, совершенные повторно или по предварительному сговору группой лиц, или если они причинили существенный вред, - наказываются лишением свободы на срок от трех до шести лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет и с конфискацией программных и технических средств, с помощью которых было совершено несанкционированное вмешательство, которые являются собственностью виновного лица.

Примечание. Значительным вредом в статьях 361-363-1, если он заключается в причинении материального ущерба, считается вред, который в сто и более раз превышает необлагаемый минимум доходов граждан.

Объектом такого преступления являются ЭВМ, АС, компьютерные сети и сети электросвязи. Объектом такого преступления также может быть право собственности на компьютерную информацию.

Для признания факта совершения преступления, состав которого предусмотрен в ст. 361 УК, суд должен установить не только совершение деяния, но и наступление хотя бы одного из указанных в законе последствий: утечки, потери, подделки, блокирования информации, искажения процесса ее обработки или нарушения установленного порядка ее маршрутизации. То есть между несанкционированным вмешательством в работу ЭВМ, АС, компьютерных сетей или сетей электросвязи должна быть причинная связь хотя бы с одним из общественно опасных последствий.

Объективная сторона преступления проявляется в форме несанкционированного вмешательства в работу ЭВМ, их систем, компьютерных сетей или сетей электросвязи, следствием которого являются:

- утечка;
- потеря;
- подделка;
- блокирование информации;
- искажение процесса обработки информации;
- нарушение установленного порядка ее маршрутизации.

Несанкционированное вмешательство в работу ЭВМ, их систем или компьютерных сетей - это проникновение в эти машины, их системы или сети и совершение действий, которые изменяют режим работы машины, ее системы или компьютерной сети, или же полностью или частично останавливают их работу, без разрешения (согласия) соответствующего собственника или уполномоченных им лиц, а также влияние на работу ЭВМ с помощью различных технических устройств, способных повредить работе машины.

Под несанкционированным вмешательством в работу сетей электросвязи следует понимать любые (кроме вмешательства в работу ЭВМ, их систем или компьютерных сетей, обеспечивающих работу сетей электросвязи) совершенные без согласия собственника соответствующей сети или должностных лиц, на которых возложено обеспечение ее нормальной работы, действия, в результате которых прекращается (приостанавливается) работа сети электросвязи или происходят изменения режима этой работы.

Поскольку запрещенное ст. 361 деяние заключается во вмешательстве в работу компьютеров и комплексов, работа которых связана с работой компьютеров, то следует считать, что информацией, о которой говорится в статье, главным образом является компьютерной информацией. Компьютерная информация - это текстовая, графическая или любая другая информация (данные), которая существует в электронном виде, сохраняется на соответствующих носителях и может создаваться, изменяться или использоваться с помощью ЭВМ. В то же время действие статьи распространяется и на передачу по каналам связи другой информации (например, передачу информации с помощью факса, телетайпа, телекса).

Частью первой ст. 361 охватываются как случаи проникновения (воздействия) в работающую ЭВМ, систему или сеть (например, проникновения в системы одного работающего персонального компьютера из такого же другого), так и несанкционированное включение неработающей машины и проникновения в нее (влияние на ее работу).

Утечка информации - это ситуация, когда информация становится известной (доступной) субъектам, не имеющим права доступа к ней, а потеря информации - ситуация, когда информация, которая ранее существовала в АС, перестает существовать для физических или юридических лиц, имеющих право собственности на нее, в полном или ограниченном объеме.

Подделка информации означает искажение информации, которая должна обрабатываться или храниться в АС, а блокирование информации - прекращение доступа к ней относительно лица, имеющего право такого доступа.

Искажение процесса обработки информации - изменение процесса обработки информации компьютером или АС, в результате которой обработка информации не дает результатов вообще, дает неверные результаты или дает лишь часть тех результатов, которые можно было получить до этого изменения.

Нарушением установленного порядка маршрутизации информации следует считать изменение режима работы сети электросвязи, в результате которого определенная информация, передаваемая в этой сети, попадает или может попасть в распоряжение лица, которое в условиях нормальной работы сети не должно было получить эту информацию.

Преступление считается законченным с момента наступления хотя бы одного из указанных в ч. 1 ст. 361 последствий.

Субъект преступления общий.

Субъективная сторона преступления характеризуется умышленной виной. Преступные действия могут быть совершены только с прямым умыслом, тогда как отношение виновного к последствиям преступления может характеризоваться как прямым, так и косвенным умыслом.

Квалифицирующими признаками (ч. 2 ст. 361) преступления является совершение его:

- повторно;
- по предварительному сговору группой лиц;
- причинения им значительного ущерба.

Понятие существенный вреда для случаев, когда он заключается в причинении материального ущерба, определено в примечании к ст. 361. Однако из содержания примечания следует, что существенный вред может иметь и нематериальный характер. Нематериальный вред в случае совершения деяний, предусмотренных статьями 361-363-1, может выражаться во временном приостановлении (прекращении) работы или другом нарушении нормального режима работы данного предприятия, организации, учреждения, их отдельных структурных подразделений, подрыве деловой репутации гражданина или юридического лица, причинении гражданину морального вреда вследствие потери, незаконного распространения или утечки информации, которая является результатом его научной или творческой деятельности и т.д. Существенный вред нематериального характера является оценочным понятием. Следовательно, вопрос о том, следует ли признать ущерб значительным, решается органами досудебного следствия, прокурором или судом с учетом конкретных обстоятельств дела.

Статья 361-1. Создание с целью использования, распространения или сбыта вредных программных или технических средств, а также их распространение или сбыт

1. Создание с целью использования, распространения или сбыта, а также распространение или сбыт вредных программных или технических средств, предназначенных для несанкционированного вмешательства в работу электронно-

вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи, - наказываются штрафом от пятисот до тысячи необлагаемых минимумов доходов граждан или исправительными работами на срок до двух лет, либо лишением свободы на тот же срок, с конфискацией программных или технических средств, предназначенных для несанкционированного вмешательства в работу электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи, которые являются собственностью виновного лица.

2. Те же действия, совершенные повторно или по предварительному сговору группой лиц, или если они причинили существенный вред, - наказываются лишением свободы на срок до пяти лет с конфискацией программных или технических средств, предназначенных для несанкционированного вмешательства в работу электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи, которые являются собственностью виновного лица.

Запрещенные данной статьей действия признаны опасными, поскольку они несут угрозу для работы ЭВМ, АС, компьютерных сетей и сетей электросвязи, а иногда и непосредственно наносят им вред. Эти действия также создают программно-технический инструментарий для совершения деяний, предусмотренных ст. 361. Поэтому основным **объектом** данного преступления следует считать нормальную работу ЭВМ, АС, компьютерных сетей и сетей электросвязи, а дополнительным факультативным объектом - право собственности на компьютерную информацию.

Предметом преступления являются вредные программные и технические средства, предназначенные для несанкционированного вмешательства в работу ЭВМ, АС, компьютерных сетей или сетей электросвязи.

Вредные программные и технические средства, операции с которыми запрещены данной статьей УК, могут быть в виде вредоносных компьютерных программ или технических устройств, которые работают с использованием таких программ. Наиболее распространенными разновидностями вредоносных программных средств, подпадающих под действие данной статьи, являются:

- компьютерные вирусы - компьютерные программы, способные после проникновения в операционную системы ЭВМ или в АС нарушить нормальную работу компьютера, АС или компьютерной сети, а также уничтожить, повредить или изменить компьютерную информацию;

- программы, предназначенные для нейтрализации паролей и других средств защиты компьютерных программ или компьютерной информации от несанкционированного доступа;

- программы-шпионы, которые после их проникновения в определенную АС, компьютерную сеть, операционную систему ЭВМ или отдельную компьютерную программу обеспечивают несанкционированный доступ постороннего лица к информации, хранящейся в ЭВМ, АС, сети или программе или незаметно для собственника или законного пользователя осуществляют несанкционированную передачу такой информации постороннему лицу.

Объективная сторона преступления заключается в:

- создании вредных программных или технических средств с целью их дальнейшего использования, распространения или сбыта;

- их распространении;

- их сбыте.

Созданием следует считать как разработку (изготовление) абсолютно нового вредоносного программного или технического средства, так и модификацию существующего средства, следствием которой является изменение его свойств.

Использование вредных программных или технических средств - это действия, направленные на использование этих средств в соответствии с их свойствами и назначением.

Распространением вредных программных или технических средств является открытие доступа к ним неопределенному кругу лиц, а также действия, в результате которых эти средства (в частности, компьютерные вирусы) начинают автоматически воспроизводиться и распространяться в ЭВМ, АС или компьютерных сетях.

Сбытом вредных программных или технических средств является осуществление любым способом платной или бесплатной передачи их в распоряжение другого лица. Сбытом следует считать и передачу копий вредных программных средств.

Преступление, совершенное в форме создания вредных программных или технических средств, является законченным с момента завершения процесса создания хотя бы одного такого средства. В случае совершения преступления в форме распространения его следует считать законченным с момента предоставления доступа к такому средству другим лицам, или же действий, после которых начинается его автоматическое воспроизведение и распространение. В случае сбыта таких средств преступление является законченным с момента передачи другому лицу хотя бы одной программы или технического устройства, которые являются вредными программными или техническими средствами.

В случае использования лицом, ранее созданного им вредоносного программного или технического средства для несанкционированного вмешательства в работу ЭВМ, АС, компьютерных сетей или сетей электросвязи такие действия, при условии наступления соответствующих последствий, должны квалифицироваться как совокупность преступлений, предусмотренных ст. 361 и ст. 361-1 УК.

Субъективная сторона данного преступления характеризуется виной в форме прямого умысла. Лицо должно осознавать вредные свойства созданного, распространенного или сбытого им программного или технического средства. Для совершения преступления в форме создания вредоносного программного или технического средства обязательным признаком субъективной стороны является цель дальнейшего использования, распространения или сбыта такого средства.

Субъект преступления общий.

Квалифицирующие признаки этого преступления совпадают с квалифицирующими признаками преступления, предусмотренного ст. 361.

Особенностью дополнительного наказания, применяемого к виновному в совершении преступления, предусмотренного данной статьей, является то, что конфискации подлежат любые принадлежащие виновному программные и технические средства, предназначенные для несанкционированного вмешательства в работу ЭВМ, АС, компьютерных сетей или сетей электросвязи, а не только те, которые были созданы, распространены или сбыты при совершении данного преступления.

Статья 361-2. Несанкционированные сбыт или распространение информации с ограниченным доступом, которая сохраняется в электронно-вычислительных машинах (компьютерах), автоматизированных системах, компьютерных сетях или на носителях такой информации

1. Несанкционированные сбыт или распространение информации с ограниченным доступом, которая хранится в электронно-вычислительных машинах (компьютерах), автоматизированных системах, компьютерных сетях или на носителях такой информации, созданной и защищенной согласно действующему законодательству, - наказываются штрафом от пятисот до тысячи необлагаемых минимумов доходов граждан или лишением свободы на срок до двух лет с конфискацией программных или технических средств, с помощью которых был осуществлен несанкционированный сбыт или распространение информации с ограниченным доступом, которые являются собственностью виновного лица.

2. Те же действия, совершенные повторно или по предварительному сговору группой лиц, или если они причинили существенный вред, - наказываются лишением свободы на срок от двух до пяти лет с конфискацией программных или технических средств, с помощью которых был осуществлен несанкционированный сбыт или распространение информации с ограниченным доступом, которые являются собственностью виновного лица.

Объектом преступления является право собственности на компьютерную информацию с ограниченным доступом.

Предметом преступления является информация с ограниченным доступом, которая хранится в ЭВМ, АС, компьютерных сетях или на носителях такой информации, то есть компьютерная информация с ограниченным доступом.

Объективная сторона преступления заключается в несанкционированном сбыте или распространении компьютерной информации с ограниченным доступом. Основной состав преступления (ч. 1 ст. 361-2) является формальным, для его наличия наступления после совершения запрещенных действий каких-то последствий не требуется.

Сбытом компьютерной информации с ограниченным доступом является ее платная или бесплатная передача хотя бы одному лицу, не имеющему доступа к этой информации, а распространением - размещение в АС или компьютерной сети с предоставлением свободного доступа к ней или иные действия, которые создают возможность свободного доступа к ней неопределенного круга лиц.

Сбыт или распространение компьютерной информации с ограниченным доступом следует считать несанкционированными, если эти действия совершены без разрешения (согласия) владельца информации. Несанкционированные сбыт

или распространение содержат признаки комментируемого преступления как в том случае, когда они совершены лицом, которому в установленном порядке был предоставлен доступ к соответствующей информации, так и в случае совершения их лицом, которое такого доступа не имело.

Несанкционированный сбыт или распространение компьютерной информации с ограниченным доступом, совершенные после получения такой информации в результате несанкционированного вмешательства в работу ЭВМ, их систем, компьютерных сетей или сетей электросвязи, образуют совокупность преступлений и должны квалифицироваться по этой статье и статье 361.

В случаях умышленного распространения или сбыта компьютерной информации, которая является государственной тайной или служебной информации, действия виновного должны квалифицироваться по данной статье и, при наличии соответствующих признаков, по статьям 111, 114, 328 или 330. В случаях совершения таких же действий относительно защищенной информации, которая является коммерческой или банковской тайной, они, при наличии соответствующих признаков, должны дополнительно квалифицироваться по ст. 231 или 232; по такой же информации, которая является врачебной тайной - по ст. 145; по соответствующей информации, которая является тайной усыновления (удочерения) - по ст. 168; по защищенной информации, которая является перепиской или иной частной корреспонденцией гражданина - по ст. 163.

Субъективная сторона преступления характеризуется прямым или косвенным умыслом.

Субъект преступления общий.

Квалифицирующие признаки этого преступления совпадают с квалифицирующими признаками преступления, предусмотренного ст. 361.

Статья 362. Несанкционированные действия с информацией, которая обрабатывается в электронно-вычислительных машинах (компьютерах), автоматизированных системах, компьютерных сетях или сохраняется на носителях такой информации, совершенные лицом, имеющим право доступа к ней

1. Несанкционированные изменение, уничтожение или блокирование информации, которая обрабатывается в электронно-вычислительных машинах (компьютерах), автоматизированных системах или компьютерных сетях или хранится на носителях такой информации, совершенные лицом, имеющим право доступа к ней, - наказываются штрафом от шестисот до тысячи необлагаемых минимумов доходов граждан или исправительными работами на срок до двух лет с конфискацией программных или технических средств, с помощью которых было совершено несанкционированные изменение, уничтожение или блокирование информации, которые являются собственностью виновного лица.

2. Несанкционированные перехват или копирование информации, которая обрабатывается в электронно-вычислительных машинах (компьютерах), автоматизированных системах, компьютерных сетях или хранится на носителях такой информации, если это привело к ее утечке, совершенные лицом, имеющим право доступа к такой информации, - наказываются лишением свободы на срок до трех лет с лишением права занимать определенные должности или заниматься

определенной деятельностью на тот же срок и с конфискацией программных или технических средств, с помощью которых было осуществлено несанкционированные перехват или копирование информации, которые являются собственностью виновного лица.

3. Действия, предусмотренные частью первой или второй настоящей статьи, совершенные повторно или по предварительному сговору группой лиц, или если они причинили существенный вред, - наказываются лишением свободы на срок от трех до шести лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет и с конфискацией программных или технических средств, с помощью которых были осуществлены несанкционированные действия с информацией, которые являются собственностью виновного лица.

Статья 363. Нарушение правил эксплуатации электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей, сетей электросвязи или порядка и правил защиты информации, которая в них обрабатывается

Нарушение правил эксплуатации электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи или порядка или правил защиты информации, в них обрабатывается, если это причинило существенный вред, совершенные лицом, отвечает за их эксплуатацию, - наказываются штрафом от пятисот до тысячи необлагаемых минимумов доходов граждан или ограничением свободы на срок до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на тот же срок.

Статья 363-1. Препятствование работе электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи путем массового распространения сообщений электросвязи

1. Умышленное массовое распространение сообщений электросвязи, осуществлено без предварительного согласия адресатов, что привело к нарушению или прекращению работы электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи, - наказывается штрафом от пятисот до тысячи необлагаемых минимумов доходов граждан или ограничением свободы на срок до трех лет.

2. Те же действия, совершенные повторно или по предварительному сговору группой лиц, если они причинили существенный вред, - наказываются ограничением свободы на срок до пяти лет или лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет и с конфискацией программных или технических средств, с помощью которых было осуществлено массовое распространение сообщений электросвязи, которые являются собственностью виновного лица.

Важным в предотвращении возможных каналов утечки информации являются и ответственность лиц допустивших нарушения предусмотренные ст. 359 и 360 УК Украины.

Статья 359. Незаконные приобретение, сбыт или использование специальных технических средств получения информации

1. Незаконное приобретение или сбыт специальных технических средств негласного получения информации, а также незаконное их использования - наказываются штрафом от двухсот до тысячи необлагаемых минимумов доходов граждан или ограничением свободы на срок до четырех лет, либо лишением свободы на тот же срок.

2. Те же действия, совершенные повторно или по предварительному сговору группой лиц, - наказываются лишением свободы на срок от четырех до семи лет.

3. Действия, предусмотренные частью первой или второй настоящей статьи, совершенные организованной группой или если они причинили существенный вред охраняемым законом правам, свободам или интересам отдельных граждан, государственным или общественным интересам или интересам отдельных юридических лиц, - наказываются лишением свободы на срок от семи до десяти лет.

Статья 360. Умышленное повреждение линий связи

Умышленное повреждение кабельной, радиорелейной, воздушной линии связи, проводного вещания или сооружений или оборудования, входящих в их состав, если оно повлекло временное прекращение связи, - наказывается штрафом от ста до двухсот необлагаемых минимумов доходов граждан или исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет.

Согласно статьи 255 Кодекса Украины об административных правонарушениях, органы Государственной службы специальной связи и защиты информации Украины вправе составлять протоколы по делам об административных правонарушениях по ст. 164 (в части, касающейся правонарушений в области хозяйственной деятельности, лицензии на проведение которой выдает эта служба), пункту 9 части первой ст. 212^2 и ст. 188^{31}.

Так, невыполнение норм и требований криптографической и технической защиты секретной информации, вследствие чего возникает реальная угроза нарушения ее конфиденциальности, целостности и доступности (п.9 ст. 212^2), - влечет наложение штрафа на граждан от одного до трех необлагаемых налогом минимумов доходов граждан и на должностных лиц – от трех до десяти необлагаемых налогом минимумов доходов граждан.

Повторное в течение года совершение нарушения из числа предусмотренных частью первой настоящей статьи, за которое лицо уже было подвергнуто административному взысканию, - влечет наложение штрафа на граждан от трех до восьми необлагаемых налогом минимумов доходов граждан и на должностных лиц – от пяти до пятнадцати необлагаемых налогом доходов граждан.

Неисполнение законных требований должностных лиц органов Государственной службы специальной связи и защиты информации Украины относительно устранения нарушений законодательства о криптографической и технической защите информации, которая является собственностью государства, или информации с ограниченным доступом, требование относительно защиты

которой установлено законом, и законодательства в сфере предоставления услуг электронной цифровой подписи, а также создание иных препятствий для исполнения возложенных на них обязанностей (ст. 188^{31}) – влекут наложение штрафа на должностных лиц от пятидесяти до ста необлагаемых налогом минимумов доходов граждан.

Те же действия, совершенные повторно на протяжении года после наложения административного взыскания , -влекут наложение штрафа на должностных лиц от ста ста пятидесяти необлагаемых минимумов доходов граждан.

В соответствии со ст. 255 Кодекса Украины об административных правонарушениях, органы Службы безопасности Украины вправе составлять протоколы по делам об административных правонарушениях в сфере технической защиты информации, предусмотренных статьями 195^{5} и 212^{6}.

Статья 195^{5}. Незаконное хранение специальных технических средств негласного получения информации

Незаконное хранение специальных технических средств негласного получения информации, - влечет наложение штрафа на граждан от пятидесяти до ста необлагаемых налогом минимумов доходов граждан с конфискацией специальных технических средств для снятия информации с каналов связи, иных средств негласного получения информации и на должностных лиц – от двухсот до пятисот необлагаемых налогом минимумов доходов граждан с конфискацией специальных технических средств для снятия информации с каналов связи, иных средств негласного получения информации.

Статья 212^{6}. Осуществление незаконного доступа к информации в информационных (автоматизированных) системах, незаконное изготовление или распространение копий баз данных информационных (автоматизированных) систем

Осуществление незаконного доступа к информации, которая хранится, обрабатывается или передается в автоматизированных системах, — влечет наложение штрафа от пяти до десяти не облагаемых налогом минимумов доходов граждан с конфискацией средств, использованных для незаконного доступа, либо без таковой.

То же действие, совершенное лицом, которое в течение года было подвергнуто административному взысканию за нарушение, предусмотренное в части первой настоящей статьи, — влечет наложение штрафа от десяти до двадцати не облагаемых налогом минимумов доходов граждан с конфискацией средств, использованных для незаконного доступа.

Что касается, дисциплинарных взысканий, то, как известно, статьей 147 Кодекса законов о труде Украины к работнику может быть применена только одна из следующих мер взыскания:

- выговор;
- увольнение.

Законодательством, уставами и положениями могут быть предусмотрены для отдельных категорий работников и другие дисциплинарные взыскания.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Конституція України від 28.06.1996 р. №254к/96-ВР [Текст] // Відомості Верховної Ради України (ВВР). – 1996. - № 30. - С. 141.
2. Цивільний кодекс України від 16.01.2003 р. №435-IV [Електронний ресурс]. - Режим доступу: http://zakon.rada.gov.ua/go/435-15.
3. Господарський кодекс України від 16.01.2003 р. №436-IV [Електронний ресурс]. - Режим доступу: http://zakon3.rada.gov.ua/laws/show/436-15.
4. Цивільний процесуальний кодекс України від 18.03.2004 №1618-IV [Електронний ресурс]. - Режим доступу: http://zakon4.rada.gov.ua/laws/show/1618-15
5. Господарський процесуальний кодекс України від 06.11.91 №1799-XII [Електронний ресурс]. - Режим доступу: http://zakon4.rada.gov.ua/laws/show/1798-12
6. Кодекс законів про працю України від 10.12.1971 р. № 322-VIII [Електронний ресурс]. - Режим доступу: http://zakon3.rada.gov.ua/laws/show/322-08.
7. Кодекс України про адміністративні правопорушення від 07.12.1984 №8073-X [Електронний ресурс]. - Режим доступу: http://zakon2.rada.gov.ua/laws/show/80731-10.
8. Про інформацію [Текст] : закон України в редакції від 13.01.2011 р. № 2938 – VI // Відомості Верховної Ради України (ВВР). – 2011. - № 32. - С. 313.
9. Про захист економічної конкуренції [Текст] : закон України від 11.01.2001 р. №2210–III // Відомості Верховної Ради України (ВВР). – 2001. - № 12. - С. 64.
10. Про доступ до публічної інформації [Текст] : закон України від 13.01.2011 р. №2939–VI // Відомості Верховної Ради України (ВВР). – 2011. - № 32. - С. 314.
11. Про державну таємницю [Текст] : закон України в редакції від 21.09.1999 р. №1079 – XIV // Відомості Верховної Ради України (ВВР). –1999. - № 49. - С. 428.
12. Про банки і банківську діяльність [Текст] : закон України від 07.12.2000 г. № 2121–III // Відомості Верховної Ради України (ВВР). – 2001. - № 5-6. - С. 30.
13. Про захист персональних даних [Текст] : закон України від 01.06.2010 г. № 2297– VI // Відомості Верховної Ради України (ВВР). – 2010. - № 34. - С. 481.
14. Про Державну службу спеціального зв’язку та захисту інформації України [Текст] : закон України від 23.02.2006 г. №3475–IV // Відомості Верховної Ради України (ВВР). – 2006. - № 30. - С. 258.
15. Про Національну систему конфіденційного зв’язку [Текст] : закон України від 10.01.2002 р. №2919–III // Відомості Верховної Ради України (ВВР). – 2002. - № 15. - С.103.
16. Про захист інформації в інформаційно-телекомунікаційних системах [Текст] : закон України від 05.07.1994 р. №80/94-ВР // Відомості Верховної Ради України (ВВР). – 1994. - № 31. - С. 286.

17. Про електронні документи та електронний документообіг [Текст] : закон України від 22.05.2003 р. №851-IV // Відомості Верховної Ради України (ВВР). – 2003. - № 36. - С. 275.
18. Положення про порядок здійснення криптографічного захисту інформації в Україні [Електронний ресурс] : наказ Президента України від 22.05.1998 г. №505/98. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/505/98
19. Положення про технічний захист інформації в Україні [Електронний ресурс] : наказ Президента України від 27.09.1999 г. №1229/99. – Режим доступу: http://zakon.rada.gov.ua/laws/show/1229/99
20. Про додержання прав людини під час проведення оперативно-технічних заходів [Електронний ресурс] : наказ Президента України від 07.11.2005 № 1556/2005. - Режим доступу: http://zakon2.rada.gov.ua/laws/show/1556/2005
21. Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію [Електронний ресурс] : постанова Кабінету Міністрів України від 27.11.1998 р. №1893. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/1893-98.
22. Концепція технічного захисту інформації в Україні [Електронний ресурс] : постанова Кабінету Міністрів України від 08.10.1997 р. №1126. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/1126-97.
23. Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, а автоматизованих системах [Електронний ресурс] : постанова Кабінету Міністрів України від 16.02.1998 р. №180. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/180-98.
24. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [Електронний ресурс] : постанова Кабінету Міністрів України від 29.03.2006 р. №373. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/373-2006.
25. Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації [Електронний ресурс] : постанова Кабінету Міністрів України від 24.06.2006 р. №868. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/868-2006.
26. Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [Електронний ресурс] : наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 04.07.2008 р. №112. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/z0690-08.
27. Інструкція про порядок постачання і використання ключів до засобів криптографічного захисту інформації [Електронний ресурс] : наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 12.06.2007 р. №114. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/z0729-07.
28. Положення про державний контроль за станом технічного захисту інформації [Електронний ресурс] : наказ Адміністрації Державної служби

спеціального зв'язку та захисту інформації України від 16.05.2007 р. №87. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/z0785-07.
29. Положення про державну експертизу в сфері технічного захисту інформації [Електронний ресурс] : наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16.05.2007 р. №93. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/z0820-07.
30. Правила проведення робіт із сертифікації засобів захисту інформації [Електронний ресурс] : наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України та Державного комітету України з питань технічного регулювання та споживчої політики від 25.04.2007 р. №75/91. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/z0498-07.
31. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі [Електронний ресурс] : Нормативний документ системи технічного захисту інформації НД ТЗІ 3.7-001-99. – Режим доступу: http://dstszi.kmu.gov.ua.
32. Тимчасове положення про категоріювання об'єктів [Електронний ресурс] : Нормативний документ системи технічного захисту інформації ТПКО-95. – Режим доступу: http://dstszi.kmu.gov.ua.
33. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу [Електронний ресурс] : Нормативний документ системи технічного захисту інформації НД ТЗІ 1.1-002-99. – Режим доступу: http://dstszi.kmu.gov.ua.
34. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу [Електронний ресурс] : Нормативний документ системи технічного захисту інформації НД ТЗІ 2.5-004-99. – Режим доступу: http://dstszi.kmu.gov.ua.
35. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу [Електронний ресурс] : Нормативний документ системи технічного захисту інформації НД ТЗІ 2.5-005-99. – Режим доступу: http://dstszi.kmu.gov.ua.
36. Типове положення про службу захисту інформації в автоматизованій системі [Електронний ресурс] : Нормативний документ системи технічного захисту інформації НД ТЗІ 1.4-001-2000. – Режим доступу: http://dstszi.kmu.gov.ua.
37. Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу [Електронний ресурс] : Нормативний документ системи технічного захисту інформації НД ТЗІ 3.6-001-2000. – Режим доступу: http://dstszi.kmu.gov.ua.
38. Вимоги до захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2 [Електронний ресурс] : Нормативний документ системи технічного захисту інформації НД ТЗІ 2.5-008-2002. – Режим доступу: http://dstszi.kmu.gov.ua.
39. Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу [Електронний ресурс] : Нормативний документ системи технічного захисту інформації НД ТЗІ 2.5-010-03. – Режим доступу: http://dstszi.kmu.gov.ua.

40. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі [Електронний ресурс] : Нормативний документ системи технічного захисту інформації НД ТЗІ 3.7-003-05. – Режим доступу: http://dstszi.kmu.gov.ua.
41. Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок [Електронний ресурс] : Нормативний документ системи технічного захисту інформації ТР ТЗІ ПЕМВН-95. – Режим доступу: http://dstszi.kmu.gov.ua.
42. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок [Електронний ресурс] : Нормативний документ системи технічного захисту інформації ТР ЕОТ - 95. – Режим доступу: http://dstszi.kmu.gov.ua.
43. Абалмазов, Э.И. Направленные микрофоны: мифы и реальность [Текст] / Э.И. Абалмазов // Специальная техника.- 1996.- №4.
44. Андрощук, Г.А. Экономическая безопасность предприятия: защита коммерческой тайны [Текст] : монография / Г.А. Андрущак, П.П. Крайнев; под ред.. А.Д. Святоцкий.- К.: ВД «Ін Юре», 2000.- 400 с.
45. Бландова, Е.С. Помехоподавляющие изделия. Рекомендации по выбору и применению [Текст] / Е.С. Бландова // Специальная техника. – 2001. - №2.
46. Бондарчук, Ю.В. Безпека бізнесу: організаційно-правові основи [Текст] : науково-практичний посібник/ Ю.В. Бондарчук, А.І. Марущак. - К.: Видавничий дім «Скіф», КНТ, 2008.- 372 с.
47. Волков, В.Г. Наголовные приборы ночного видения [Текст] / В.Г. Волков // Специальная техника.- 2002.- №5.
48. Гнилицкая, Л.В. Теоретико-методологические и прикладные основы обеспечения экономической безопасности субъектов хозяйственной деятельности [Текст] : монография / Л.В, Гнилицкая, А.И. Захаров, П.Я. Пригунов.- К.: Дорадо-Друк, 2011.- 290 с.
49. Доценко, С.М. Безопасность оптоволоконных кабельных систем [Текст] / С.М. Доценко // Конфидент. – 1999. - №6.
50. Економічна безпека підприємства [Текст]: навч. посіб. (для студ. вищих навч. закл.) / Т.М. Іванюта, А.О. Заїчковський. – К.: Центр учбової літератури, 2009.- С. 256.
51. Зінченко Л. Коммерческая тайна предприятия [Текст] / Л. Зинченко // Ваш бизнес.- 2011. - № 9.
52. Ионкин, П.А. Теоретические основы электротехники. Том I. Основы теории цепей. / Под ред. П.А. Ионкина. М.: Высшая школа, 1976.
53. Комментарии к ЗУ «О защите персональных данных» № 2297-VI [Електронний ресурс].– Режим доступа:http://uriskonsult.ucoz.ru/news/kommentarii_k_zu_o_zashhite_personalnykh_dannykh_2297_vi_dalee_zakon_2297_vi/2011-12-24.
54. Крутов, В.В. Становлення та розвиток недержавної системи безпеки підприємництва [Текст] : монографія / В.В. Крутов.- К.: Фенікс, 2008.- 406 с.

55. Крысин, А.В. Безопасность предпринимательской деятельности [Текст]: навч. посіб. (для студ. вищих навч. закл.) / А.В. Крысин. – М.: Финансы и статистика, 1996.- С. 256.
56. Кузнєцов, И.Н. Учебник по информационно-аналитической работе [Текст] / И.Н. Кузнецов.- М.: Яуза, 2001.- 320 с.
57. Ліпкан, В.А. Національна безпека України [Текст] : навч. посібник / В.А. Ліпкан.- К.: Кондор, 2008.- 552 с.
58. Ліпкан, В.А. Національна безпека України [Текст] : навч. посібник / В.А. Ліпкан.- К.: КНТ, 2009.- 576 с.
59. Луспеник, Д. Раскрытие банковской тайны [Текст] / Д. Луспеник, З. Мельник // Юридическая практика.- 2010. - № 7 (634).
60. Марущак, А.І. Правові основи захисту інформації з обмеженим доступом [Текст] : курс лекцій / А.І. Марущак.- К.: КН, 2007.- 208 с.
61. Микроэлектронные устройства автоматики [Текст] : учеб. пособие для вузов / А.А. Сазонов, А.Ю. Лукичев, В.Т. Николаев и др.; под ред. А.А. Сазонова. – М.: Энергоатомиздат, 1991. – 384 с.
62. Минаев, Г.А. Образование и безопасность [Текст] : учеб. пособие / Г.А. Минаев.- М.: ЛОГОС, 2009.- 312 с.
63. Організаційно-правові основи захисту інформації з обмеженим доступом [Текст] : навч. посібник / За заг. ред.. проф.. В.С. Сідака.- К.:Вид-во Європейського ун-ту, 2006.- 232 с.
64. Организационно-правовые основы защиты информации с ограниченным доступом [Текст]: учеб. пособие / А.Б. Стоцкий, О.И. Тимошенко, А.М. Гуз и др.; под общ. ред. В.С. Сидак, П.Я. Прыгунов. – К.: Изд-во Европейского ун-та, 2005.- С.
65. Підприємництво та правовий захист комерційної таємниці [Текст]: навч.-практ. посіб. для вищих навч. закл. / Г.К. Нікіфоров, С.С. Нікіфоров. – К.: Олан, 2001.- С. 208.
66. Промышленный шпионаж – угроза экономической безопасности предприятия (фирмы) [Текст]: курс лекций / Антирейдерский союз предпринимателей Украины. Консультационный центр «Корпоративная безопасность предприятия (фирмы)». - Библиотека Антирейдера.
67. Рекомендации по организации защиты коммерческой тайны в ИЭС им. Е.О. Патона. Научный руководитель В.Н. Суриков. – К., 1991.
68. Саликов, В.Л. Приборы ночного видения: история поколений [Текст] / В.Л. Саликов // Специальная техника.- 2000.- №2.
69. Соснин, А.С. Менеджмент безопасности предпринимательства [Текст] : учеб. пособие / А.С. Соснин, П.Я. Пригунов.- К.: Изд-во Европейского ун-та, 2002.- 504 с.
70. Соснин, А.С. Менеджмент безопасности предпринимательства [Текст] : учеб. пособие / А.С. Соснин, П.Я. Пригунов.- К.: Изд-во Европейского ун-та, 2004.- 357 с.
71. Технические средства и методы защиты информации [Текст] : учебник для ВУЗов / А.П. Зайцев, А.А. Шелупанова, Р.В. Мещеряков и др.; под ред. А.П.

Зайцева и А.А. Мещерякова. – М.: ООО «Издательство Машиностроение», 2009. – 508 с.
72. Торокин, А.А. Инженерно-техническая защита информации [Текст] : учеб. пособие для студентов, обучающихся по специальностям в обл. информ. безопасности / А.А. Торокин. – М.: Гелиос АРВ, 2005. – 960 с.
73. Управління фінансово-економічною безпекою [Текст] : навч. посібник / О.А. Кириченко, С.М. Лаптєв, П.Я. Пригунов та ін.; за ред.. чл..-кор. АПН України, к.юр.н., д.іст.н., професора В.С. Сідака.- К.: Дорадо-Друк, 2010.- 480 с.
74. Хорев, А.А. Технические каналы утечки акустической (речевой) информации [Текст] / А.А. Хореев // Специальная техника.- 1998.- №1.
75. Хореев, А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации [Текст] : учеб. пособие / А.А. Хорев. – М.: Гостехкомиссия Росси, 1998. – 320 с.
76. Штейншлегер, В.Б. Неленейное рассеяние радиоволн металлическими объектами [Текст] / В.Б. Штейншлегер // Успехи физических наук. – 1984.- т.142, вып. 1. –с. 131.
77. Ярочки, В.И. Служба безопасности коммерческого предприятия [Текст] / В.И. Ярочкин.- К.: Изд-во «Ось-89», 2005.
78. http://www.yukonoptics.ru
79. http://www.vsebinokli.ru
80. http://www.bnti.ru
81. http://www. laborkomplekt.ru
82. http://www.pdamix.ru
83. http://www.profinfo.ru/catalog/r33/118.html
84. http://www.spymarket.com/prod/recom/shtml
85. http://www.info-protect.ru
86. http://www.mascom.ru/article255.asp.htm
87. http://www.infosecur.ru
88. http://www.brandcenter.ru
89. http://www.sbchel.ru/content/it/po/secretnet/

Научное издание

Солодкий Владимир Сергеевич

Тимофеев Владимир Александрович

Технические средства защиты информации с ограниченным доступом

Редактор
О.И. Солодкая

Компьютерная верстка
Н.В. Помогалова