Федеральное агентство по образованию

Государственное образовательное учреждение
высшего профессионального образования

Владимирский государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

КНИГА 13

А.И. СОКОЛОВ, М.Ю. МОНАХОВ

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Технические каналы утечки информации

Учебное пособие

Владимир 2007

УДК 004.056
ББК 32.97
С59

Редактор серии – доктор технических наук, профессор
М.Ю. Монахов

Рецензенты:

Кандидат технических наук, доцент
зав. кафедрой оперативно-технической деятельности
Владимирского юридического института
К.Н. Курысев

Кандидат технических наук, доцент
Владимирского государственного университета
А.А. Воронин

Печатается по решению редакционно-издательского совета
Владимирского государственного университета

С59 **Соколов, А. И**. Технические средства защиты информации: технические каналы утечки информации : учеб. пособие / А. И. Соколов, М. Ю. Монахов ; Владим. гос. ун-т. – Владимир : Изд-во Владим. гос. ун-та, 2006. – 71 с. (Комплексная защита объектов информатизации. Кн. 13 / под ред. М. Ю. Монахова).
ISBN 5-89368-715-9

Это тринадцатая книга из серии «Комплексная защита объектов информатизации». В ней представлен систематизированный материал по основным методам и средствам формирования технических каналов утечки информации.

Учебное пособие предназначено для студентов специальности 090104 – комплексная защита объектов информатизации дневной формы обучения.

Ил. 38. Табл. 1. Библиогр.: 27 назв.

УДК 004.056
ББК 32.97

ISBN 5-89368-715-9

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ 4

Глава 1. ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ...7

Глава 2. КЛАССИФИКАЦИЯ И ХАРАКТЕРИСТИКА ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ ОСНОВНЫМИ И ВСПОМОГАТЕЛЬНЫМИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ 16

Глава 3. КЛАССИФИКАЦИЯ И ХАРАКТЕРИСТИКА ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ АКУСТИЧЕСКОЙ ИНФОРМАЦИИ 26

Глава 4. КЛАССИФИКАЦИЯ И ХАРАКТЕРИСТИКА ТЕХНИЧЕСКИХ КАНАЛОВ ПЕРЕХВАТА ИНФОРМАЦИИ ПРИ ЕЕ ПЕРЕДАЧЕ ПО КАНАЛАМ СВЯЗИ 45

Глава 5. ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ВИДОВОЙ ИНФОРМАЦИИ....52

Глава 6. МАТЕРИАЛЬНО-ВЕЩЕСТВЕННЫЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ 59

Глава 7. КОМПЛЕКСИРОВАНИЕ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ....62

КОНТРОЛЬНЫЕ ВОПРОСЫ И ЗАДАНИЯ 66

ЗАКЛЮЧЕНИЕ....68

БИБЛИОГРАФИЧЕСКИЙ СПИСОК 70

ПРЕДИСЛОВИЕ

Современный этап развития российского общества характеризуется существенным возрастанием роли и актуальности проблем обеспечения безопасности всех сфер жизнедеятельности. Особенно показателен этот процесс для безопасности информационной сферы, которая за последнее десятилетие вышла из области компетенции специальных служб госструктур на уровень взаимоотношений в обществе.

Один из основных источников угроз информационной безопасности – противозаконная деятельность зарубежных разведок, конкурентов, преступных сообществ, организаций, групп, формирований и отдельных лиц, направленная на сбор или хищение ценной (конфиденциальной) информации, закрытой для доступа посторонних лиц. Причем в последние годы приоритеты подобной деятельности смещаются и в экономическую область.

Главной причиной возникновения промышленного (экономического) шпионажа является стремление к реализации конкурентного преимущества – важнейшего условия достижения успеха в рыночной экономике. Охота за чужими секретами позволяет компаниям экономить собственные средства на ведение НИОКР и фундаментальные исследования, быть в курсе дел конкурентов, использовать их научно-технические достижения.

В условиях ожесточенной конкурентной борьбы на рынке масштабы промышленного шпионажа резко возрастают. Все шире используются плоды научно-технического прогресса. Шпионаж становится гибче, изощреннее и аморальнее.

В последние годы промышленный шпионаж превращается в весьма доходную разновидность бизнеса. В нашей стране промышленный шпионаж осуществляется в целях овладения рынками сбыта, подделки товаров, дискредитации или устранения (экономи-

ческого или физического подавления) конкурентов, срыва переговоров по контрактам, перепродажи фирменных секретов, шантажа определенных лиц, создания условий для подготовки и проведения террористических и диверсионных акций.

На рынке России представлен арсенал самых современных технических средств промышленного шпионажа, которые находят все более широкое применение на практике. К ним относятся: визуально-оптические, фотографические, телевизионные, тепловизионные (инфракрасные), акустические, радио-, радиотехнические и другие средства разведки.

Для организации защиты конфиденциальной информации необходимо знать возможности технических средств промышленного шпионажа, способы их применения и, в первую очередь, представлять себе каналы, по которым ценная информация потенциально может быть перехвачена, то есть возможна ее утечка.

Утечка информации означает несанкционированный перенос информации от ее источника к злоумышленнику по каналу утечки информации. Если утечка информации происходит с помощью технических средств, то соответствующий канал называется техническим каналом утечки информации.

Технический канал утечки информации – совокупность объекта разведки (источник информации), технического средства разведки (средство перехвата информации), с помощью которых добывается информация об этом объекте, и физической среды, в которой распространяется информационный сигнал (канал связи).

По сути, под техническим каналом утечки информации понимают способ получения разведывательной информации об объекте с помощью технических средств, а под разведывательной информацией – обычно сведения или совокупность данных об объекте разведки независимо от формы их представления.

Материальными носителями информации являются сигналы – некоторые физические процессы, с помощью которых передаются информационные сообщения. По своей физической природе сигналы могут быть электрическими, электромагнитными, акустическими и т. д. То есть сигналы, как правило, – это электромагнитные, механические и другие виды колебаний, в которых информация записана на изменяемых ею параметрах, например, в амплитуде, частоте, фазе, длине волны и т. д.

Сигналы распространяются в определенных физических средах. В общем случае средой распространения могут быть воздушные, жидкостные и твердые среды, например, воздушное пространство, конструкции зданий, соединительные линии, токопроводящие элементы, грунт (земля) и т. п.

Технические средства разведки служат для приема сигналов в каналах утечки информации и выделения из них информационных параметров, а также создания самих технических каналов утечки информации.

В учебном пособии даны классификация и характеристики технических каналов утечки информации, обрабатываемой техническими средствами, передаваемой по каналам связи, а также акустической (речевой), видовой (оптической) и материально-вещественной информации. Рассмотрены методология и способы несанкционированного съема информации с объектов разведки.

Глава 1. ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ

Информация, записанная на распространяющихся в пространстве носителях, может быть перенесена этими носителями от источника к несанкционированному получателю. В таком случае говорят об утечке информации по аналогии с утечкой жидких или газообразных веществ. Однако по сравнению с ними утечка информации имеет ряд особенностей.

1.1. Общие сведения

Под утечкой информации понимается несанкционированный процесс переноса информации от источника к злоумышленнику (зарубежной разведке, конкурентам, криминалу, террористам и т. д.).

Понятие «утечка» широко распространено. Говорят об утечке воды, газа, материальных ценностей со склада, информации из различных структур и т. п. Утечка информации возможна путем ее разглашения людьми, утерей последними носителей с информацией, а также при ее переносе с помощью полей, потоков элементарных частиц, веществ в газообразном, жидком или твердом виде. Например, желание сотрудников поделиться последними новостями о работе с родными или близкими создает возможности (предпосылки) утечки конфиденциальной информации. Переносчиками информации могут быть любые ее носители.

Часто под утечкой понимают случайный процесс, вроде вытекания воды из неисправного крана. Такой подход представляется упрощенным. В криминальной практике известны факты организации утечки, например, бензина с последующим списыванием его на случайную неисправность в нефтепроводе или хранилище. В политической жизни общества практикуется «организация утечки»

информации из правительственных структур с целью зондирования или подготовки общественного мнения перед принятием непопулярных решений.

Утечка информации по сравнению с утечкой (хищением) материальных объектов имеет ряд особенностей, которые надо учитывать при организации защиты информации:

– утечка информации может происходить только при попадании ее к заинтересованному в ней несанкционированному получателю (злоумышленнику), в отличие, например, от утечки воды или газа;

– при утечке информации происходит ее тиражирование, которое не изменяет характеристики исходного носителя информации (не уменьшается количество листов документа, не сокращается число пикселей изображения, не меняются размеры, цвет и другие демаскирующие признаки продукции и т. д.);

– цена информации при ее утечке уменьшается за счет тиражирования;

– утечка возникает, если принятые меры по обеспечению безопасности информации недостаточны, неэффективны или несвоевременны, а факт утечки информации, как правило, обнаруживается спустя некоторое время, по последствиям.

Первая особенность имеет существенное значение для безопасности информации, так как сами по себе факты утери документа, разглашения сведений, распространения носителей за пределы контролируемой зоны и другие действия далеко не всегда приводят к утечке информации. Например, если конфиденциальный разговор во время совещания в кабинете руководителя организации слышен в приемной из-за неплотно закрытой двери, а в приемной нет людей, то утечки информации нет, хотя носитель информации (акустическая волна) выходит за пределы контролируемой зоны – помещения. Если в приемной находится добросовестно выполняющий свои обязанности секретарь руководителя, который после совещания будет оформлять его результаты, то утечка информации также отсутствует, так как информация не попадет к злоумышленнику. Только в том случае, когда в приемной будет находиться сотрудник организации или посетитель, который воспользуется информацией из услышанного разговора в личных целях или поделится ею с другими заинтересованными в ней людьми, происходит утечка информации из кабинета руководителя. То есть можно говорить об утечке информации как факте нарушения ее бе-

зопасности только тогда, когда она попадает к злоумышленнику независимо от того, знает или не знает об этом владелец информации. Если по какой-либо причине на этом пути передачи информации происходит разрыв в цепочке и информация исчезает на носителе или вместе с ее носителем, то утечки информации не происходит.

Следовательно, под утечкой следует понимать не процесс распространения носителя информации за пределы определенной области пространства вообще, а частный случай распространения, когда информация попадает к злоумышленнику. Выход же носителя за пределы заданной области создает предпосылки для утечки информации и повышает угрозу ее безопасности.

Замечание о несанкционированности получателя имеет принципиальное значение. Если получатель информации санкционирован, то речь идет не об утечке, а о передаче информации по так называемому функциональному каналу связи, специально создаваемому для обеспечения коммуникаций в человеческом обществе.

Часто хищение и утечку информации рассматривают как автономные процессы. Если под хищением понимать умышленное присвоение чужой собственности без разрешения ее законного владельца, то утечка информации представляет собой один из способов ее хищения. Действительно, если человек на государственной земле находит клад, слиток из драгоценных металлов или драгоценный камень, которые по закону являются собственностью государства, то он обязан их сдать соответствующему государственному органу. В противном случае его действия классифицируются как хищение и он может быть привлечен к ответственности. Аналогичная ситуация с утечкой информации. Когда злоумышленник находит утерянный документ с грифом «Секретно» и сознательно продает его зарубежной спецслужбе, то он привлекается к уголовной ответственности за хищение государственной тайны.

Физический путь переноса информации от ее источника к несанкционированному получателю называется *каналом утечки*. Если запись информации на носитель канала утечки и съем ее с носителя осуществляется с помощью технических средств, то такой канал называется *техническим каналом утечки*.

Несанкционированный перенос информации полями различной природы, макро- и микрочастицами выполняется в рамках технических каналов утечки информации.

1.2. Характеристики технических каналов утечки информации

Для передачи информации носителями в виде полей и микрочастиц по любому техническому каналу (функциональному или каналу утечки) последний должен содержать три основных элемента: *источник сигнала, среду распространения носителя* и *приемник*. Обобщенная типовая структура канала передачи информации приведена на рис. 1.

Рис. 1. Структура канала передачи информации

На вход канала поступает информация в виде первичного сигнала. Первичный сигнал представляет собой носитель с информацией от ее источника или с выхода предыдущего канала. В качестве источника сигнала могут быть:

– объект наблюдения, отражающий электромагнитные и акустические волны;

– объект наблюдения, излучающий собственные (тепловые) электромагнитные волны или побочные электромагнитные излучения;

– приемо-передатчик функционального канала связи и сам канал связи;

– закладное устройство;

– источник опасного сигнала;

– источник акустических волн, модулированных информацией.

Указанные на рис. 1 стрелками пути входа и выхода информации обозначают вход и выход первичных сигналов с информацией. Так как информация от источника поступает на вход канала на языке источника (в виде буквенно-цифрового текста, символов, знаков, звуков, сигналов и т. д.), то передатчик преобразует эту форму представления информации в форму, обеспечивающую запись ее на носитель информации, соответствующий среде распространения. Кроме того, он выполняет следующие функции:

– создает (генерирует) поля (акустическое, электромагнитное) или электрический ток, которые переносят информацию;

– осуществляет запись информации на носитель (модуляцию информационных параметров носителя);

– усиливает мощность сигнала (носителя с информацией);

– обеспечивает передачу (излучение) сигнала в среду распространения в заданном секторе пространства.

Информация записывается путем изменения параметров носителя в соответствии с уровнем первичного сигнала, поступающего на вход. Если носителями информации являются субъекты и материальные тела (макрочастицы), то передатчик соответствует первоначальному смыслу этого слова – передавать или переносить, т. е. выполняет функцию носителя. В случае когда информацию переносят сигналы (поля, электрический ток и элементарные частицы), передатчики являются их источниками.

Источниками сигналов могут быть как источники функциональных каналов связи, так и опасных сигналов. К последним относятся сигналы с конфиденциальной информацией, появление которых является для источника информации случайным событием и им не контролируется.

Среда распространения носителя – часть пространства, в которой перемещается носитель. Она характеризуется набором физических параметров, определяющих условия перемещения носителя информации. Из них основными параметрами, которые надо учитывать при анализе среды распространения носителя, являются следующие:

– физические препятствия для субъектов и материальных тел;

– мера ослабления (или пропускания энергии) сигнала на единицу длины;

– частотная характеристика (неравномерность ослабления частотных составляющих спектра сигнала);

– вид и мощность помех для сигнала.

Приемник выполняет функции, обратные функциям передатчика. Он осуществляет:

– выбор (селекцию) носителя с нужной получателю информацией;

– усиление принятого сигнала до значений, обеспечивающих съем информации;

– съем информации с носителя (демодуляцию, декодирование);

– преобразование информации в форму сигнала, доступную получателю (человеку, техническому устройству), и его усиление до значений, необходимых для безошибочного восприятия информации получателем.

Если получатель информации человек, то информация с выхода приемника должна быть представлена на языке общения людей; если техническое устройство, то форма представления информации должна быть ему понятна. Например, если получатель – ЭВМ, то с выхода приемника на ЭВМ подается двоичная последовательность в кодах, например таблицы ASCII.

Канал утечки информации отличается от функционального канала передачи получателем информации. Если получатель санкционированный, то канал функциональный, в противном случае – канал утечки. Классификация каналов утечки информации дана на рис. 2.

Физическая природа носителя является основным классификационным признаком технических каналов утечки информации. По этому признаку они делятся:

– на оптические;

– радиоэлектронные;

– акустические;

– материально-вещественные.

Носитель информации в оптическом канале – электромагнитное поле в диапазоне 0,46 – 0,76 мкм (видимый свет) и 0,76 – 13 мкм (инфракрасные излучения).

В радиоэлектронном канале утечки информации в качестве носителей используются электрические, магнитные и электромагнитные поля в радиодиапазоне, а также электрический ток, распространяющийся по проводникам из меди, железа, алюминия. Диапазон колебаний этого вида носителя чрезвычайно велик: от звукового диапазона до десятков ГГц. Часто этот канал называют электромагнитным, что представляется недостаточно корректным, так как носителями информации в оптическом канале являются также электромагнитные поля, но в более высокочастотном диапазоне. Кроме того, широко используется в качестве носителя информации модулированный поток электронов (электрический ток). Объединяя эти два носителя информации в канале одного вида, целесообразно

назвать его «радиоэлектронный» (электромагнитное поле в радиодиапазоне и электроны электрического тока).

Рис. 2. Классификация каналов утечки информации

Носителями информации в акустическом канале являются механические акустические волны в инфразвуковом (менее 16 Гц), звуковом (16 – 20 кГц) и ультразвуковом (свыше 20 кГц) диапазонах частот, распространяющиеся в атмосфере, воде и твердой среде.

В материально-вещественном канале утечка информации возможна через несанкционированное распространение за пределы организации вещественных носителей с секретной или конфиденциальной информацией, прежде всего выбрасываемых черновиков документов и использованной копировальной бумаги, забракованных деталей и узлов, демаскирующих веществ. Последние в виде твердых, жидких и газообразных отходов или промежуточных продуктов содержат химические элементы, по которым в принципе можно определить состав, структуру и свойства новых материалов или восстановить технологию их получения.

Когда речь идет о распространении за пределы организации отходов производства в широком смысле, то следует отличать технический канал утечки от агентурного, в рамках которого носитель с информацией выносится проникшим к источнику злоумышленником, завербованным сотрудником организации или сотрудником, стремящимся продать информацию любому ее покупателю. Граница между каналами достаточно условна, однако при утечке информации в агентурном канале переносчиком информации является лицо, сознающее противоправные действия, а в техническом материально-веществен-

ном канале носители вывозятся из организации с целью освобождения ее от отходов или отходы распространяются в результате действия природных сил. В качестве таких сил могут быть воздушные потоки, разносящие газообразные отходы, или водные потоки рек или водоемов, куда сбрасываются недостаточно очищенные жидкие или взвешенные в воде твердые частицы демаскирующих веществ.

Каждый из технических каналов имеет свои особенности, которые необходимо знать и учитывать для обеспечения эффективной защиты информации от утечки или ее предпосылок.

По информативности каналы утечки делят на информативные, малоинформативные и неинформативные (информативность канала оценивается ценностью передаваемой по нему информации). *По времени проявления* – на постоянные, периодические и эпизодические. В постоянном канале утечка информации носит достаточно регулярный характер. Например, наличие в кабинете источника опасного сигнала может привести к передаче из кабинета речевой информации до момента обнаружения этого источника. Периодический канал утечки может возникнуть во время пролетов разведывательных космических аппаратов, при условии, например, размещения во дворе неукрытой продукции, демаскирующие признаки которой составляют тайну. К эпизодическим относят каналы, утечка информации в которых имеет разовый, случайный характер.

Канал утечки информации, состоящий из передатчика, среды распространения и приемника, является одноканальным. Однако возможны варианты, когда утечка информации происходит более сложным путем – по нескольким последовательным или параллельным каналам. При этом используется свойство информации переписываться с одного носителя на другой. Например, если в кабинете ведется конфиденциальный разговор, то утечка возможна не только по акустическому каналу через стены, двери, окна, но и по оптическому – путем съема информации лазерным лучом со стекла окна или по радиоэлектронному с использованием установленной в кабинете радиозакладки. В двух последних вариантах образуется составной канал, образованный из последовательно соединенных акустического и оптического (на лазерном луче) или акустического и радиоэлектронного (радиозакладка – среда распространения – радиоприемник) каналов. Для повышения дальности канала утечки может также использоваться ретранслятор, совмещающий функции

приемника одного канала утечки информации и передатчика следующего канала. Например, для повышения дальности подслушивания с использованием радиозакладки можно разместить ретранслятор в портфеле, сдаваемом в камеру хранения закрытого предприятия.

Как любой канал связи, канал утечки информации характеризуется следующими основными показателями:

– пропускной способностью;

– дальностью передачи информации.

Пропускная способность канала связи оценивается количеством информации, передаваемой по нему в единицу времени с определенным качеством. В теории связи пропускная способность канала в бодах (битах в секунду) определяется по формуле

$$C = \Delta F \log_2 (1+P_с/P_п),$$

где ΔF – ширина полосы пропускания канала связи; $P_с$ и $P_п$ – мощность сигнала и помехи (в виде белого шума) в полосе пропускания канала соответственно.

Следовательно, пропускная способность канала связи является интегральной характеристикой, учитывающей как ширину полос частот сигнала, которую пропускает канал, так и его энергетику. Чем меньше отношение мощностей сигнала и помехи, тем больше ошибок в принятом сообщении и тем меньше количество переданной информации.

По ширине полосы частот пропускания каналы делят на узко- и широкополосные. Стандартный телефонный канал для передачи речевой информации имеет полосу 300 – 3400 Гц и относится к узкополосным, а канал для передачи телевизионных сигналов шириной 8 МГц – к широкополосным. Чем шире канал, тем больше информации можно передать за единицу времени. Так как для добывания информации с требуемым качеством необходимо обеспечить на входе приемника канала минимально допустимое для каждого вида информации и носителя отношение сигнал/помеха, то это отношение достигается на различном удалении от источника сигнала в зависимости от мощности сигнала и помехи, а также величины (коэффициента) ослабления (затухания) сигнала в канале. Носители информации существенно отличаются по величине затухания в среде распространения: в наибольшей степени уменьшается энергия акустической волны, в наименьшей – электромагнитная волна в длинноволновом диапазоне частот.

Глава 2. КЛАССИФИКАЦИЯ И ХАРАКТЕРИСТИКА ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ ОСНОВНЫМИ И ВСПОМОГАТЕЛЬНЫМИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

2.1. Общие сведения

Технические средства и системы приема, обработки, хранения, отображения и передачи информации (ТСПИ) по отношению к информации ограниченного доступа подразделяются на основные и вспомогательные.

Под *основными техническими средствами и системами (ОТСС)* понимают технические средства и построенные на их базе системы, непосредственно обрабатывающие (принимающие, хранящие, обрабатывающие и передающие) конфиденциальную информацию. К таким средствам относятся: электронно-вычислительная техника, режимные АТС, системы оперативно-командной и громкоговорящей связи, звукоусиления, звукового сопровождения и звукозаписи и другие, предназначенные для ведения конфиденциальных переговоров и обработки иной конфиденциальной информации.

При выявлении технических каналов утечки информации ОТСС необходимо рассматривать как систему, включающую основное, а также каналообразующее, коммуникационное (стационарное или мобильное) оборудование, оконечные устройства, соединительные линии (совокупность проводов и кабелей, прокладываемых между отдельными ОТСС и их элементами), распределительные и коммутационные устройства.

Часто вместе с ОТСС устанавливаются технические средства и системы, непосредственно не участвующие в обработке конфиденциальной информации, но использующиеся совместно с основны-

ми техническими средствами. Такие технические средства и системы называются *вспомогательными техническими средствами и системами (ВТСС)*. К ним относятся: технические средства и линии открытой телефонной, громкоговорящей связи, системы пожарной и охранной сигнализации, системы электропитания, электроосвещения, заземления, радиофикации, электробытовые и электроизмерительные приборы и т. д. При этом всегда возникает задача защиты информации – разместить ВТСС по отношению к ОТСС так, чтобы информационные наводки электромагнитного поля ОТСС на ВТСС были минимальными и безопасными. В свою очередь, информация в ОТСС защищается инженерно-техническими, программно-аппаратными, криптографическими, режимными и другими мерами.

Для создания технических каналов утечки информации наибольший интерес представляют соединительные линии ОТСС и ВТСС, имеющие выход за пределы *контролируемой зоны (КЗ)*, т. е. зоны, в которой исключено появление лиц и транспортных средств, не имеющих постоянных или временных пропусков.

Кроме соединительных линий ОТСС и ВТСС за пределы контролируемой зоны могут выходить провода и кабели, к ним не относящиеся, но проходящие через помещения, где установлены технические средства, а также металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции. Такие провода, кабели и токопроводящие элементы, подверженные информационным наводкам ПЭМИ ОТСС, называются *посторонними проводниками*, или *распределенными антеннами*, и также подлежат защите от утечки.

В зависимости от физической природы возникновения информационных сигналов, а также среды их распространения и способов перехвата, технические каналы утечки информации, обрабатываемой ОТСС, делят на электромагнитные, электрические, параметрические и вибрационные.

На рис. 3 приведена классификация технических каналов утечки информации, обрабатываемой основными техническими средствами и системами.

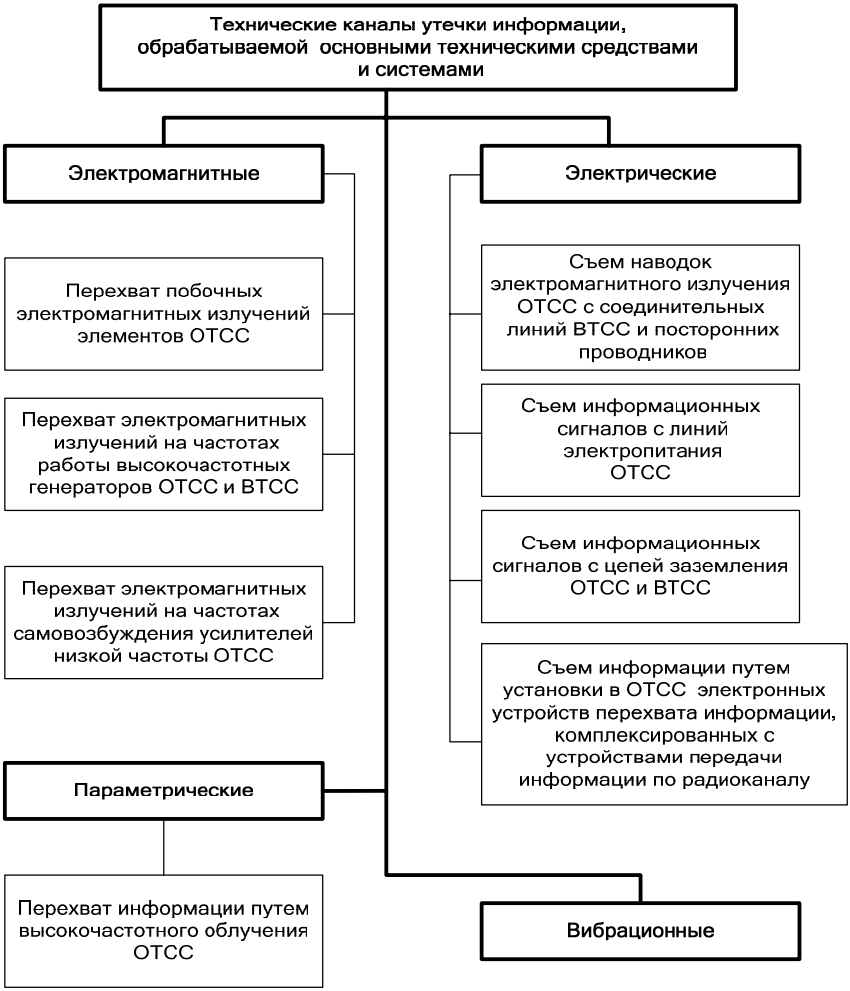

Рис. 3. Классификация технических каналов утечки информации, обрабатываемой основными техническими средствами и системами

2.2. Электромагнитные каналы утечки информации

К электромагнитным относят каналы утечки информации, возникающие за счет различного вида побочных электромагнитных излучений (ПЭМИ) основных технических средств и систем:

– элементов ОТСС;

– на частотах работы высокочастотных генераторов ОТСС и ВТСС;

– на частотах самовозбуждения усилителей низкой частоты ОТСС.

Электромагнитные излучения элементов ОТСС. В ОТСС носителем информации является электрический ток, параметры которого (амплитуда, частота и фаза) изменяются по закону информационного сигнала. При прохождении электрического тока по токоведущим элементам ОТСС и вокруг них (в окружающем пространстве) возникают электрическое и магнитное поля. В силу этого элементы ОТСС можно рассматривать как излучатели электромагнитного поля, модулированного информационным сигналом.

Электромагнитные излучения на частотах работы высокочастотных генераторов ОТСС и ВТСС. В состав ОТСС и ВТСС могут входить различного рода высокочастотные генераторы. К таким устройствам можно отнести:

– задающие генераторы;

– генераторы тактовой частоты;

– генераторы стирания и подмагничивания магнитофонов;

– гетеродины радиоприемных и телевизионных устройств;

– генераторы измерительных приборов и т. д.

В результате внешних воздействий информационного сигнала (например электромагнитных колебаний) на элементах высокочастотных генераторов наводятся электрические сигналы. Наведенные электрические сигналы могут вызвать непреднамеренную модуляцию собственных высокочастотных колебаний генераторов. Эти промодулированные высокочастотные колебания излучаются в окружающее пространство. Приемником магнитного поля могут быть катушки индуктивности колебательных контуров, дроссели в цепях электропитания и т. д. Приемником электрического поля являются провода высокочастотных цепей и другие элементы ВТСС и ОТСС.

Электромагнитные излучения на частотах самовозбуждения усилителей низкой частоты ОТСС. К усилителям низкой частоты в ОТСС относят усилители систем звукоусиления и звукового сопровождения, магнитофонов, систем громкоговорящей связи и т. п. Их самовозбуждение возможно за счет случайных преобразований отрицательных обратных связей (индуктивных или емкостных) в паразитные положительные, что приводит к переводу усилителя из режима усиления в режим автогенерации сигналов. Частота самовозбуждения лежит в пределах рабочих частот нелинейных элементов усилителей низкой частоты (например, полупроводниковых приборов, электровакуумных ламп и т. п.). Сигнал на частотах самовозбуждения, как правило, оказывается промодулированным информационным сигналом. Самовозбуждение наблюдается, в основном, при переводе усилителя в нелинейный режим работы, т. е. в режим перегрузки.

Перехват побочных электромагнитных излучений ОТСС осуществляется средствами радио-, радиотехнической разведки, размещенными в том числе вне контролируемой зоны.

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

Схема электромагнитных каналов утечки информации представлена на рис. 4.

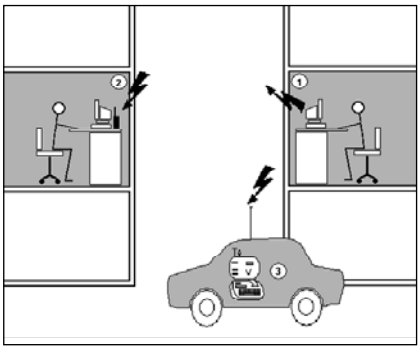

Рис. 4. Перехват побочных электромагнитных излучений: 1 – пользователь ПЭВМ, излучающей ПЭМИ при обработке конфиденциальной информации; 2 – разведчик в другом помещении (доме), перехватывающий ПЭМИ с целью выделить исходную конфиденциальную информацию; 3 – разведчик на транспортном средстве, перехватывающий ПЭМИ с целью выделить исходную конфиденциальную информацию

2.3. Электрические каналы утечки информации

Причинами возникновения электрических каналов утечки информации могут быть:

– наводки электромагнитных излучений ОТСС на соединительные линии ВТСС и посторонние проводники, выходящие за пределы контролируемой зоны;

– просачивание информационных сигналов в линии электропитания ОТСС;

– просачивание информационных сигналов в систему заземления ОТСС;

– использование закладных устройств.

Наводки электромагнитных излучений ОТСС возникают при излучении элементами ОТСС информационных сигналов, а также при наличии гальванической связи соединительных линий ОТСС и посторонних проводников или линий ВТСС. Уровень наводимых сигналов В значительной степени зависит от мощности излучаемых сигналов, расстояния до проводников, а также длины совместного пробега соединительных линий ОТСС и посторонних проводников.

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

Случайной антенной является цепь ВТСС или посторонние проводники, способные принимать побочные электромагнитные излучения элементов ОТСС. Различают сосредоточенные и распределенные случайные антенны .

Сосредоточенная случайная антенна представляет собой компактное техническое средство, например, телефонный аппарат, громкоговоритель радиотрансляционной сети и т. д.

К распределенным случайным антеннам относят случайные антенны с распределенными параметрами: кабели, провода, металлические трубы и другие токопроводящие коммуникации.

Просачивание информационных сигналов в линии электропитания. Это возможно при наличии магнитной связи между выходным трансформатором усилителя (например усилителя низкой частоты) и трансформатором блока питания. 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 линию электропитания также в результате того, что среднее значение потребляемого тока в оконечных каскадах усилителей зависит от амплитуды информационного сигнала, что создает неравномерную нагрузку на выпрямитель и приводит к изменению потребляемого тока по закону изменения информационного сигнала.

Просачивание информационных сигналов в систему заземления. Кроме заземляющих проводников, служащих для непосредственного соединения ОТСС с контуром заземления, гальваническую связь с землей могут иметь различные проводники, выходящие за пределы контролируемой зоны: нулевой провод сети электропитания, экраны (металлические оплетки и 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 которую могут просачиваться информационные сигналы. Кроме того, в грунте вокруг заземляющего устройства возникает электромагнитное поле, которое также является источником информации.

Перехват информационных сигналов по электрическим каналам утечки возможен путем непосредственного подключения к соединительным линиям ОТСС, ВТСС и посторонним проводникам, проходящим через помещения, где установлены ОТСС, а также к их системам электропитания и заземления. Для этих целей используются специальные средства радио- и радиотехнической разведки, а также специальная измерительная аппаратура.

Схемы электрических каналов утечки информации представлены на рис. 5 и 6.

Съем информации с использованием аппаратных закладок. В последние годы участились случаи съема информации, обрабатываемой в ОТСС, путем установки в них электронных устройств перехвата информации – *закладных устройств*.

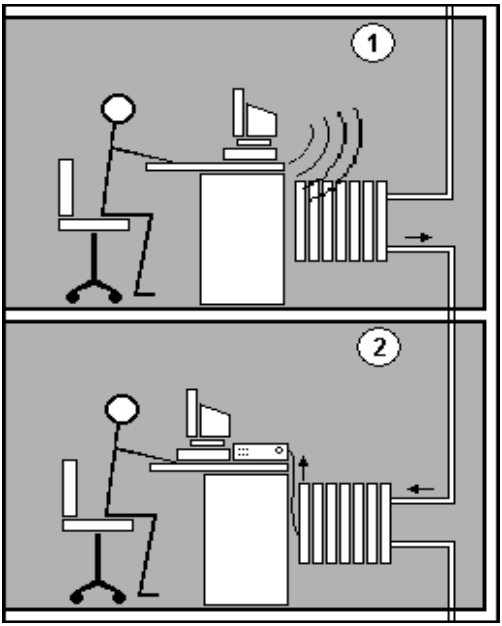

Рис. 5. Съем наводок информационных сигналов с соединительных линий ВТСС и посторонних проводников: 1 – пользователь обрабатывает информацию на ПЭВМ, расположенной вблизи постороннего проводника, на котором создаются электрические наводки от побочного электромагнитного излучения ПЭВМ; 2 – разведчик в соседнем помещении осуществляет съем наводок от ПЭМИ ПЭВМ и выделяет из них исходную информацию

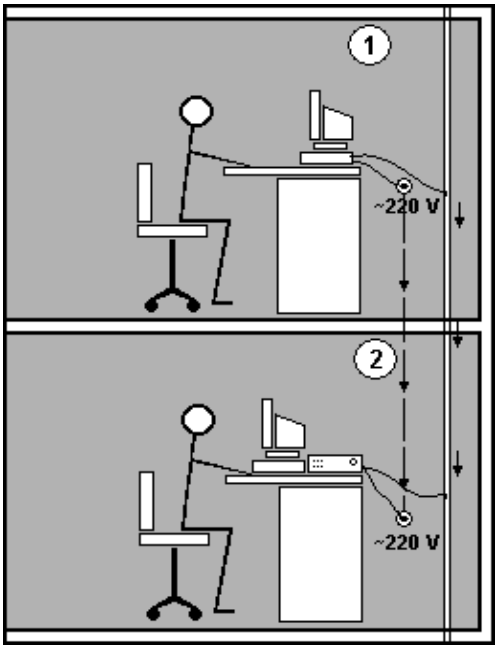

Рис. 6. Съем информационных сигналов с цепей заземления и электропитания: 1 – пользователь работает на ПЭВМ, информационные сигналы которой просачиваются в линии электропитания и заземления; 2 – разведчик в соседнем помещении подключился к линиям электропитания и заземления и снимает просочившиеся из ПЭВМ помещения 1 информационные сигналы

Электронные устройства перехвата информации, устанавливаемые в ОТСС, иногда называют *аппаратными закладками*. Они представляют собой мини-передатчики, излучение которых модулируется информационным сигналом. Наиболее часто закладки устанавливаются в технические средства иностранного производства, однако возможна их установка и в отечественных средствах.

Перехваченная с помощью закладных устройств информация или непосредственно передается по радиоканалу, или сначала записывается на специальное запоминающее устройство, а уже затем по команде передается на запросивший ее объект. Схема канала утечки информации с использованием закладных устройств представлена на рис. 7.

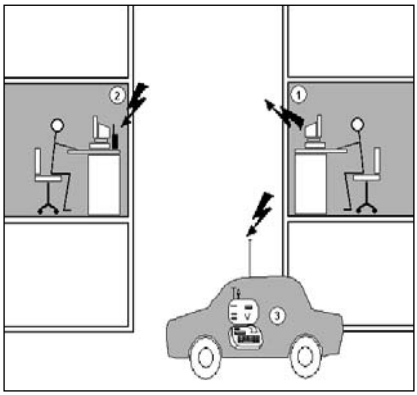

Рис. 7. Съем информации путем установки в ТСПИ аппаратных закладок: 1 – пользователь обрабатывает информацию на ПЭВМ, «оснащенной» аппаратной закладкой с передачей по радиоканалу; 2 – разведчик из соседнего помещения (дома) осуществляет прием радиосигнала закладки ПЭВМ и выделяет из него снятую информацию; 3 – разведчик из транспортного средства осуществляет прием радиосигнала закладки ПЭВМ и выделяет из него снятую информацию

2.4. Параметрические каналы утечки информации

Перехват обрабатываемой в технических средствах информации возможен также путем их «высокочастотного облучения». При взаимодействии облучающего электромагнитного поля с элементами ОТСС происходит переизлучение электромагнитного поля. В ряде случаев это вторичное излучение модулируется информационным сигналом. При съеме информации для исключения взаимного влияния облучающего и переизлученного сигналов может использоваться их временная или частотная развязка. Например, для облучения ОТСС возможно применение импульсных сигналов.

При переизлучении параметры исходного облучающего сигнала изменяются модулирующими информационными сигналами ОТСС. Поэтому данные каналы утечки информации часто называют *параметрическими*.

Для перехвата информации по данным каналам необходимы специальные высокочастотные генераторы с антеннами, имеющими узкие диаграммы направленности и специальные радиоприемные устройства. Схема параметрического канала утечки информации представлена на рис. 8.

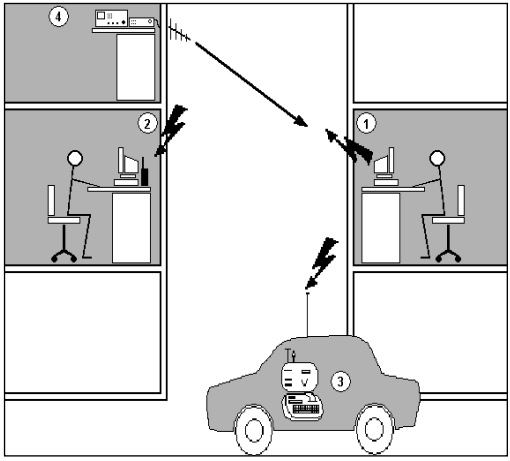

Рис. 8. Перехват информации путем «высокочастотного облучения» ТСПИ: 1 – пользователь обрабатывает конфиденциальную информацию на ТС, подверженном направленному облучению мощным ВЧ-сигналом. В ТС он модулируется конфиденциальной информацией и переизлучается; 2 – разведчик принимает переизлученный модулированный ВЧ-сигнал из соседнего помещения (дома); 3 – разведчик принимает переизлученный модулированный ВЧ-сигнал из транспортного средства; 4 – помещение с устройством направленного ВЧ-облучения ТС

2.5. Вибрационные каналы

Некоторые ТСПИ имеют в своем составе печатающие устройства, для которых можно найти соответствие между распечатываемым символом и его акустическим образом. Данный принцип лежит в основе канала утечки информации по вибрационному каналу.

Глава 3. КЛАССИФИКАЦИЯ И ХАРАКТЕРИСТИКА ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ АКУСТИЧЕСКОЙ ИНФОРМАЦИИ

3.1. Общие сведения

Под акустической понимается информация, носителем которой являются акустические сигналы. Если источник информации – человеческая речь, акустическая информация называется речевой.

Не подлежит сомнению, что наивысшую ценность представляет информация, передаваемая устно. Это объясняется рядом специфических особенностей, свойственных речи. Устно сообщают сведения, которые не могут быть доверены техническим средствам передачи. Информация, полученная в момент ее озвучивания, является самой оперативной. Живая речь, несущая эмоциональную окраску личностного отношения к сообщению, позволяет составить психологический портрет человека. Кроме того, современные методы дают возможность однозначно идентифицировать личность говорящего.

Эти особенности объясняют неослабевающий интерес противоборствующих сторон к непосредственному прослушиванию речи, циркулирующей в помещениях, по виброакустическому и акустическому (воздуховоды, окна, потолки, трубопроводы) каналам. Поэтому при решении вопросов по защите от утечки информации по техническим каналам защите речевой информации уделяется первоочередное внимание.

Акустический сигнал представляет собой возмущения упругой среды, проявляющиеся в возникновении акустических колебаний различной формы и длительности. Механические колебания частиц упругой среды, распространяющиеся от источника колебаний в окружающее пространство в виде волн различной длины, называются *акустическими.*

Первичные источники акустических колебаний – механические колебательные системы, например органы речи человека, а вторичные – преобразователи различного типа, в том числе акустоэлектрические. Последние – это устройства, предназначенные для преобразования акустических колебаний в электрические и обратно: микрофоны, телефоны, громкоговорители и другие.

В зависимости от формы акустических колебаний различают тональные и сложные сигналы. Тональный – это сигнал, вызываемый колебанием, совершающимся по синусоидальному закону. Сложный сигнал включает в себя целый спектр гармонических составляющих.

Речевой сигнал является сложным акустическим сигналом в диапазоне частот от 200 – 300 Гц до 4 – 6 кГц.

В зависимости от физической природы возникновения информационных сигналов, среды распространения акустических колебаний и способов их перехвата технические каналы утечки акустической (речевой) информации можно разделить на воздушные, виброакустические, акустоэлектрические, оптико-электронные и параметрические (рис. 9).

3.2. Воздушные технические каналы утечки информации

В воздушных технических каналах утечки информации средой распространения акустических сигналов является воздух, и для их перехвата используются миниатюрные высокочувствительные и специальные направленные микрофоны. Схемы воздушных технических каналов утечки информации показаны на рис. 10 – 15.

Миниатюрные микрофоны объединяются с портативными звукозаписывающими устройствами (диктофонами) или специальными миниатюрными передатчиками. Автономные устройства, конструкционно объединяющие миниатюрные микрофоны и передатчики, называют *закладными устройствами перехвата речевой информации, или акустическими закладками.*

Перехваченная закладными устройствами речевая информация может передаваться по радиоканалу, оптическому каналу (в инфракрасном диапазоне длин волн), по сети переменного тока, соединительным линиям ВТСС, посторонним проводникам (трубам водоснабжения и канализации, металлоконструкциям и т. п.).

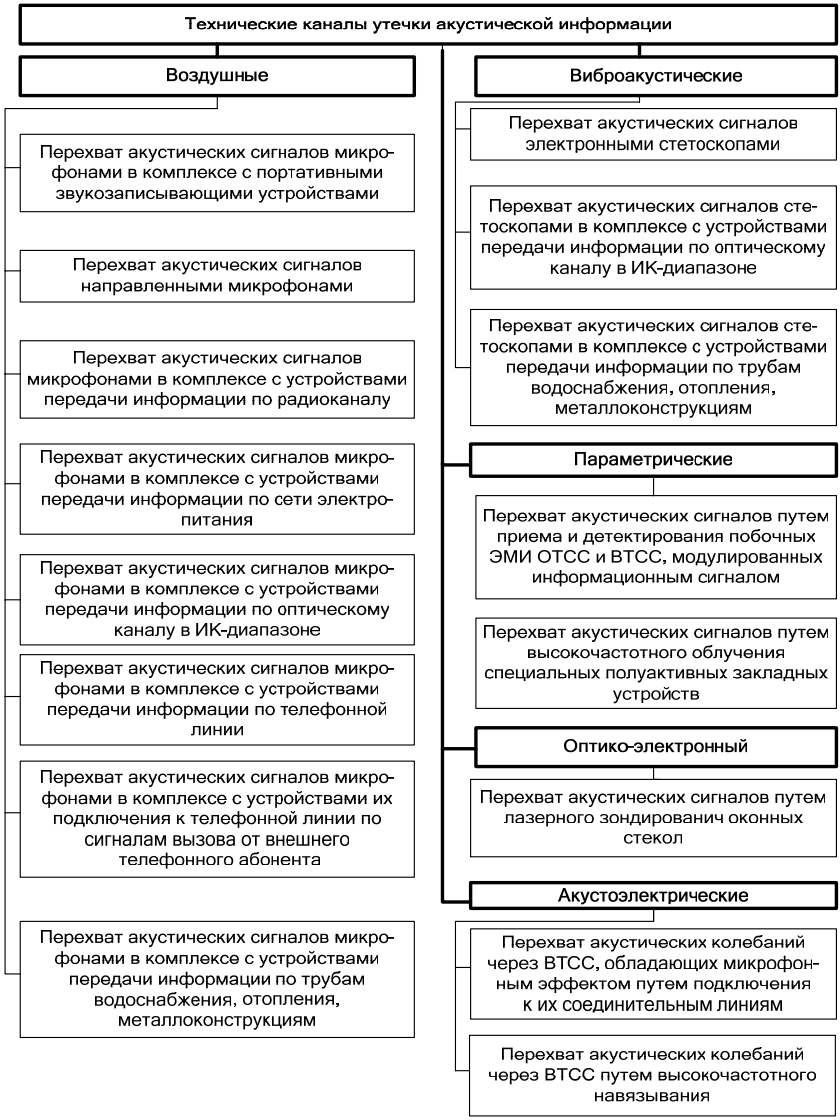

Рис. 9. Классификация технических каналов утечки акустической (речевой) информации

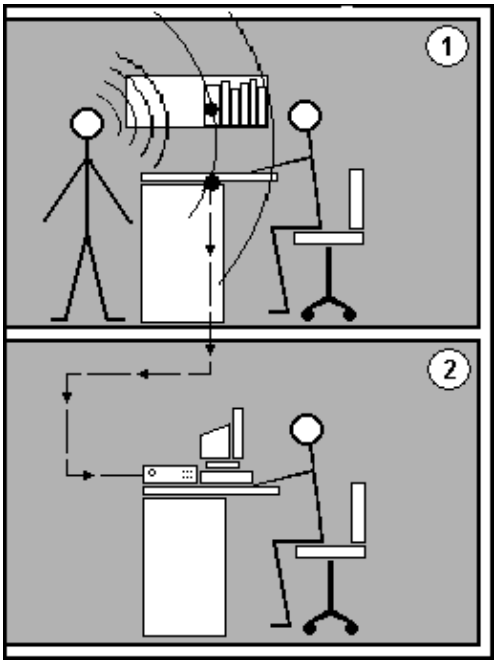

Рис. 10. Перехват акустических сигналов микрофонами, комплексированными с портативными устройствами звукозаписи: 1 – помещение, в котором происходит обмен речевой информацией, «оснащено»: закамуфлированным в книжной полке портативным микрофоном с автономным устройством звукозаписи; – скрытно установленным в письменном столе микрофоном с сигнальным кабелем, входящим в соседнее помещение; 2 – разведчик подключил устройство звукозаписи и прослушивания к сигнальному кабелю от микрофона в соседнем помещении и осуществляет перехват речевой информации

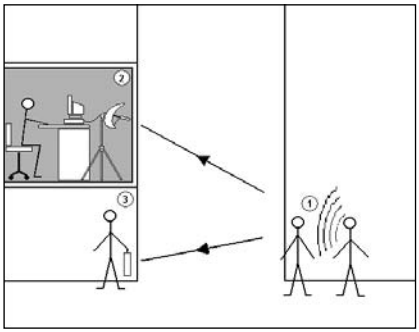

Рис. 11. Перехват акустических сигналов направленными микрофонами: 1 – собеседники осуществляют обмен речевой информацией; 2 – разведчик в соседнем помещении применяет направленный микрофон для перехвата речевой информации; 3 – разведчик применяет закамуфлированный под «дипломат» направленный микрофон для перехвата речевой информации

Причем для передачи информации по трубам и металлоконструкциям могут использоваться не только электромагнитные, но и механические ультразвуковые колебания.

Прием информации, передаваемой закладными устройствами, осуществляется, как правило, на специальные приемные устройства, работающие в соответствующем диапазоне длин волн.

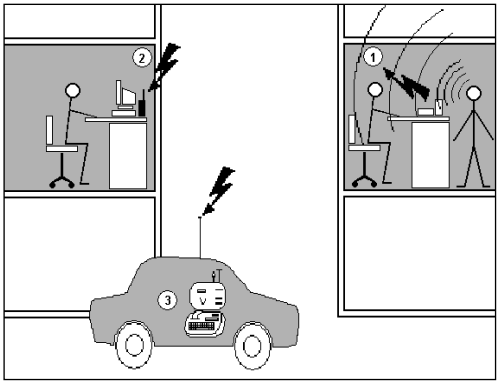

Рис. 12. Перехват акустических сигналов микрофонами, комплексированными с устройствами передачи информации по радиоканалу: 1 – в помещении, скрытно «оснащенном» радиозакладкой (микрофоном с микропередатчиком) в одном из настольных предметов, идет обмен речевой информацией; 2 – разведчик в соседнем помещении (доме) принимает радиосигнал закладки, модулированный речевой информацией помещения; 3 – разведчик в транспортном средстве принимает радиосигнал закладки, модулированный речевой информацией помещения

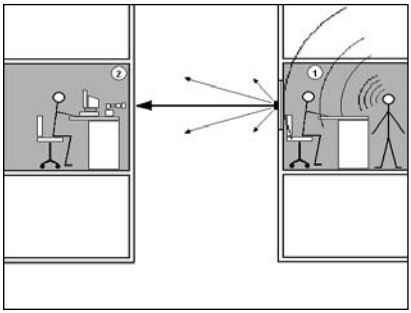

Рис. 13. Перехват акустических сигналов микрофонами (в том числе контактными), комплексированными с устройствами передачи информации по оптическому каналу: 1 – в помещении, «оснащенном» установленным на окне контактным микрофоном с микропередатчиком оптического (ИК) диапазона, происходит обмен речевой информацией; 2 – разведчик в здании напротив окна принимает сигнал оптического (ИК) микрорадиопередатчика, модулированный речевой информацией от контактного микрофона

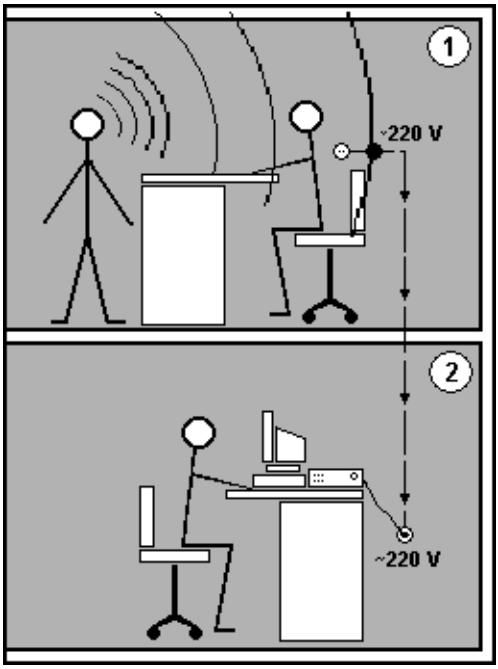

Рис. 14. Перехват акустических сигналов микрофонами, комплексированными с устройствами передачи информации по электросети: 1 – в помещении, «оснащенном» микрофоном с устройством передачи сигнала по электросети 220 В, происходит обмен речевой информацией; 2 – разведчик в соседнем помещении подключил к сети 220 В оборудование съема информационного сигнала от электросетевого закладного устройства в помещении 1 и прослушивает разговор

Рис. 15. Перехват акустических сигналов микрофонами, комплексированными с устройствами их подключения к телефонной линии («телефону-наблюдателю») по сигналам вызова от внешнего абонента: 1 – помещение, в котором происходит обмен речевой информацией, «оснащено» телефоном, в который скрытно установлен микрофон с усилителем и устройством его подключения к телефонной линии по сигналу вызова с телефона абонента-разведчика; 2 – разведчик осуществляет скрытный вызов-подключение закладного устройства телефона в помещении 1 и перехват речевой информации из помещения (прослушивание со своего телефона и запись)

Однако встречаются закладные устройства, принимать информацию с которых можно с обычного телефонного аппарата. Такие устройства устанавливаются или непосредственно в корпусе телефонного аппарата, находящегося в контролируемом помещении и называемом «телефоном-наблюдателем», или подключаются к телефонной линии, чаще всего в телефонной розетке. Подобное устройство конструкционно объединяет миниатюрный микрофон и специальный блок коммутации и обычно называется «телефонным ухом». Блок коммутации подключает микрофон к телефонной линии при дозвоне по определенной схеме до «телефона-наблюдателя» или подаче в линию специального кодированного сигнала.

Использование портативных диктофонов и акустических закладок требует проникновения на контролируемый объект (в помещение). В том случае, когда это не удается, для перехвата речевой информации используются направленные микрофоны.

3.3. Виброакустические технические каналы утечки информации

В виброакустических (структурных) технических каналах утечки информации средой распространения акустических сигналов являются конструкции зданий, сооружений (стены, потолки, полы), трубы водоснабжения, отопления, канализации и другие твердые тела. Для перехвата акустических колебаний в этом случае используются контактные микрофоны (стетоскопы). Схемы виброакустических технических каналов утечки информации представлены на рис. 16 и 17.

Контактные микрофоны, соединенные с электронным усилителем называют *электронными стетоскопами.*

По виброакустическому каналу также возможен перехват информации с использованием закладных устройств. В основном для передачи информации используется радиоканал, поэтому такие устройства часто называют *радиостетоскопами*. Возможно использование закладных устройств с передачей информации по оптическому каналу в ближнем инфракрасном диапазоне длин волн, а также по ультразвуковому каналу (по металлоконструкциям здания).

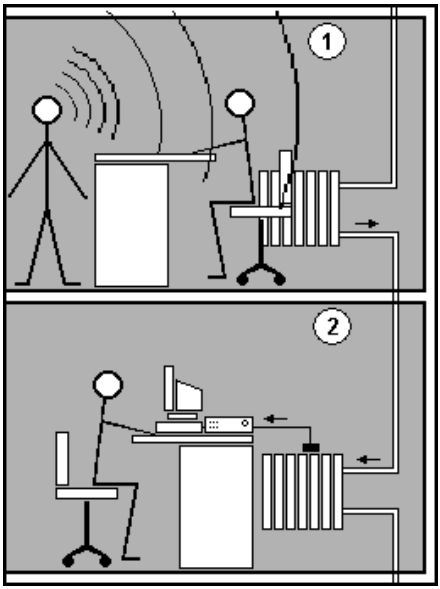

Рис. 16. Перехват виброакустического сигнала электронным стетоскопом: 1 – в помещении происходит обмен речевой информацией вблизи незащищенной акустопроводящей конструкции, в которой возникает речевой виброканал; 2 – разведчик стетоскопом, установленным на акустопроводящую конструкцию, перехватывает речевой вибросигнал

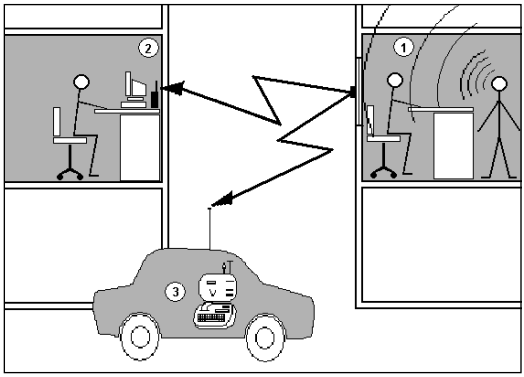

Рис. 17. Перехват акустических (речевых) сигналов электронными стетоскопами, комплексированными с устройствами передачи информации: 1 – в помещении, «оснащенном» установленным на окне радиостетоскопом (контактным микрофоном с микрорадиопередатчиком), происходит обмен речевой информацией; 2 – разведчик в соседнем помещении (доме) принимает сигнал микрорадиопередатчика, модулированный речевой информацией от стетоскопа; 3 – разведчик в транспортном средстве принимает сигнал микрорадиопередатчика, модулированный речевой информацией от стетоскопа

3.4. Акустоэлектрические технические каналы утечки информации

Акустоэлектрические технические каналы утечки информации возникают за счет акустоэлектрических преобразований акустических сигналов в электрические и включают перехват электроакустических сигналов из ВТСС, обладающих собственным «микрофонным эффектом» (рис. 18), а также получивших его путем «высокочастотного навязывания» (рис. 19).

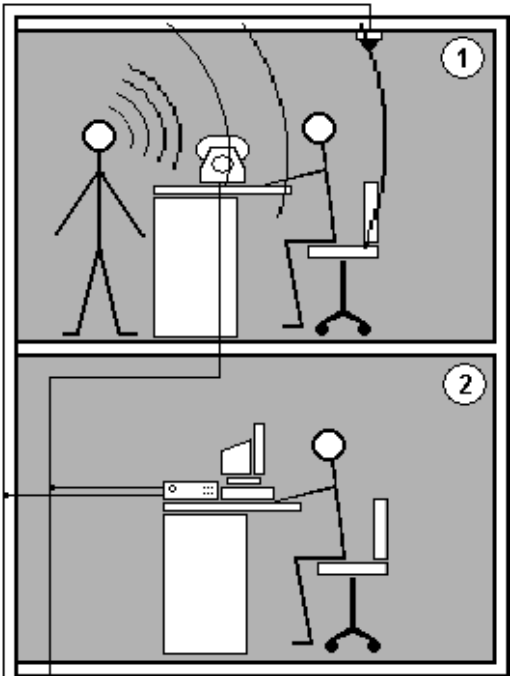

Рис. 18. Перехват акустических (речевых) сигналов через ВТСС, обладающие «микрофонным эффектом»: 1 – помещение, в котором происходит обмен речевой информацией, «оснащено»: незащищенным датчиком пожарной сигнализации и незащищенным телефоном, обладающими «микрофонным эффектом»; 2 – разведчик подключил высокочувствительный усилитель к соединительным линиям датчика пожарной сигнализации и телефона и перехватывает речевую информацию в помещении из их акустоэлектрических сигналов

Некоторые элементы ВТСС, в том числе трансформаторы, катушки индуктивности, электромагниты вторичных электрочасов, звонков телефонных аппаратов, дроссели ламп дневного света, электрореле и т. п., обладают свойством изменять свои параметры (емкость, индуктивность, сопротивление) под действием акустического поля, создаваемого источником акустических колебаний.

Изменение параметров приводит либо к появлению на данных элементах электродвижущей силы (ЭДС), изменяющейся по закону

воздействующего информационного акустического поля, либо к модуляции токов, протекающих по этим элементам, информационным сигналом. Например, акустическое поле воздействует на якорь электромагнита вызывного телефонного звонка и вызывает его колебание.

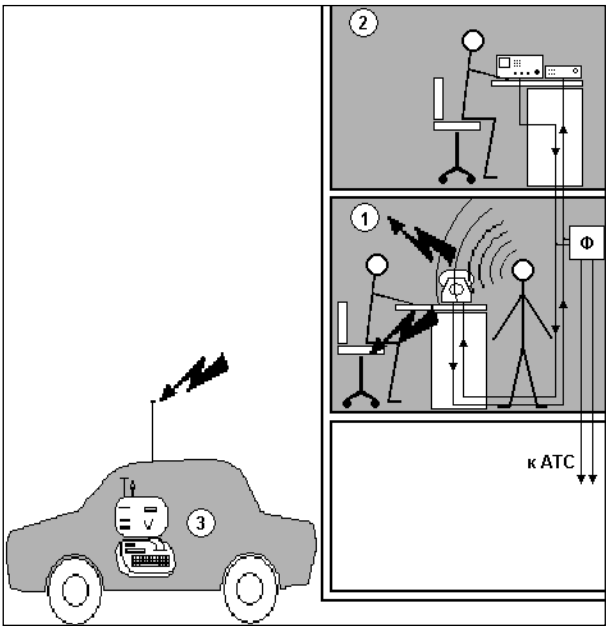

Рис. 19. Перехват акустических (речевых) сигналов через ВТСС путем «высокочастотного навязывания»: 1 – в помещении, «оснащенном» телефонным аппаратом, на который через линию подается ВЧ-генерация «навязывания», ведется обмен речевой информацией; 2 – разведчик в соседнем помещении подключил к телефонной линии генератор ВЧ-сигнала «навязывания» и выделяет из нее свой отраженный от телефонного аппарата ВЧ-сигнал, модулированный «микрофонным эффектом» от речи говорящих; 3 – разведчик в транспортном средстве принимает ВЧ-излучение «навязывания», модулированное речевой информацией от «микрофонного эффекта» телефонного аппарата в помещении 2

В результате изменяется магнитный поток сердечника электромагнита, что вызывает появление ЭДС самоиндукции в катушке звонка, изменяющейся по закону акустического поля.

ВТСС кроме указанных элементов могут содержать непосредственно акустоэлектрические преобразователи. К таким ВТСС относятся некоторые типы датчиков охранной и пожарной сигнализации, громкоговорители ретрансляционной сети и т. д. Эффект акустоэлектрического преобразования в специальной литературе называют «микрофонным эффектом». Причем из ВТСС, обладающих «микрофонным эффектом», наибольшую чувствительность к акустическому полю имеют абонентские громкоговорители и некоторые датчики пожарной сигнализации.

Перехват электроакустических колебаний в данном канале утечки информации осуществляется путем непосредственного подключения к соединительным линиям ВТСС специальных высокочувствительных низкочастотных усилителей. Например, подключая такие средства к соединительным линиям телефонных аппаратов с электромеханическими вызывными звонками, можно прослушивать разговоры, ведущиеся в помещениях, где установлены эти аппараты.

Технический канал утечки информации путем *«высокочастотного навязывания»* может быть осуществлен несанкционированным контактным введением токов высокой частоты от соответствующего генератора в линии (цепи), имеющей функциональные связи с нелинейными или параметрическими элементами ВТСС, на которых происходит модуляция высокочастотного сигнала информационным. Информационный сигнал в данных элементах ВТСС появляется вследствие акустоэлектрического преобразования акустических сигналов в электрические. В силу того, что нелинейные или параметрические элементы ВТСС для высокочастотного сигнала, как правило, представляют собой несогласованную нагрузку, промодулированный высокочастотный сигнал будет отражаться от нее и распространяться в обратном направлении по линии или излучаться. Для приема излученных или отраженных высокочастотных сигналов применяются специальные приемники с достаточно высокой чувствительностью. Для исключения влияния зондирующего и переотраженного сигналов могут использоваться импульсные сигналы «высокочастотного навязывания».

Наиболее часто такой канал утечки информации используется для перехвата разговоров, ведущихся в помещении, через телефонный аппа-рат, имеющий выход за пределы контролируемой зоны. Для исключения воздействия высокочастотного сигнала на аппаратуру АТС, в линию, идущую в ее сторону, устанавливается специальный высокочастотный фильтр.

3.5. Оптико-электронный технический канал утечки информации

Оптико-электронный (лазерный) канал утечки акустической информации образуется при облучении лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей (стекол окон, картин, зеркал и т. п.). Отраженное лазерное излучение (диффузное или зеркальное) модулируется по амплитуде и фазе (по закону вибрации поверхности) и принимается приемником оптического (лазерного) излучения, при демодуляции которого выделяется речевая информация (рис. 20). Причем лазерные приемники оптического излучения могут быть установлены в одном или разных местах (помещениях).

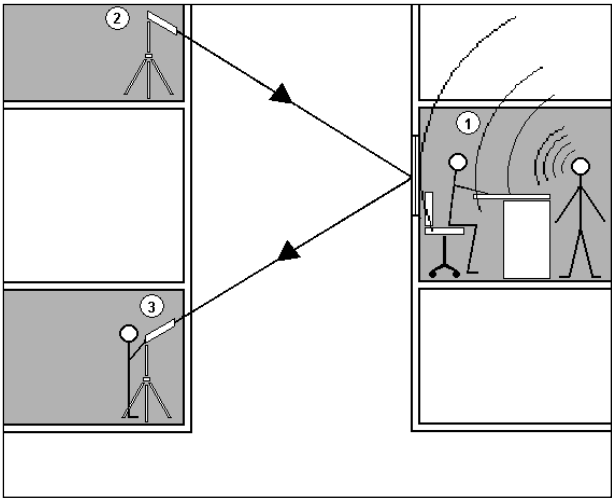

Рис. 20. Перехват акустических (речевых) сигналов путем лазерного зондирования оконных стекол: 1 – в помещении происходит обмен речевой информацией. Под воздействием акустических колебаний возникает вибрация оконного стекла; 2 – разведчик в помещении соседнего дома установил оптический лазер и навел его луч на оконное стекло; 3 – разведчик в соседнем доме принимает отраженный от окна лазерный луч, модулированный речевой информацией от вибрации оконного стекла

Для перехвата речевой информации по данному каналу используются сложные лазерные акустические локационные системы, иногда называемые *«лазерными микрофонами»*. Работают они, как правило, в ближнем инфракрасном диапазоне волн.

3.6. Параметрические технические каналы утечки информации

В результате воздействия акустического сигнала меняется давление на все элементы высокочастотных генераторов ОТСС и ВТСС. При этом изменяется (незначительно) взаимное расположение элементов схем, проводов в катушках индуктивности, дросселей и т. п., что может привести к изменениям параметров собственных высокочастотных сигналов ОТСС и ВТСС, например к модуляции воздействующим информационным акустическим сигналом.

Поэтому такой канал утечки информации называется *параметрическим.* Это обусловлено тем, что незначительное изменение взаимного расположения, например проводов в катушках индуктивности (межвиткового расстояния), приводит к изменению их индуктивности, а следовательно, к изменению частоты излучения генератора, т. е. к частотной модуляции сигнала. Или воздействие акустического поля на конденсаторы приводит к изменению расстояния между пластинами и, следовательно, изменению его емкости, что, в свою очередь, также приводит к частотной модуляции высокочастотного сигнала генератора. Наиболее часто наблюдается паразитная модуляция акустическим информационным сигналом излучений гетеродинов радиоприемных и телевизионных устройств, находящихся в выделенных помещениях и имеющих конденсаторы переменной емкости с воздушным диэлектриком в колебательных контурах гетеродинов. Промодулированные информационным сигналом высокочастотные колебания излучаются в окружающее пространство и могут быть перехвачены и детектированы средствами радиоразведки (рис. 21).

Параметрический канал утечки информации может быть реализован и путем *«высокочастотного облучения»* помещения, где установлены полуактивные переизлучающие закладные устройства, имеющие элементы, некоторые параметры которых (например добротность и резонансная частота объемного резонатора) изменяются по закону изменения воздействующего акустического (речевого) сигнала (рис. 22).

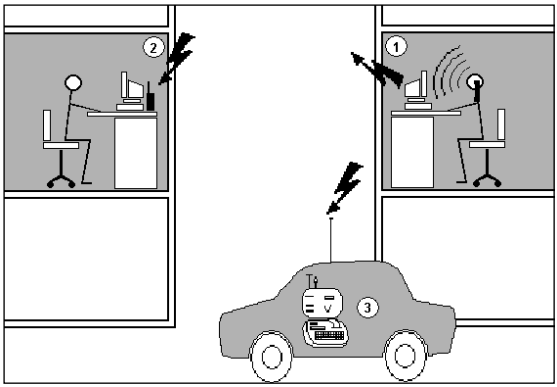

Рис. 21. Перехват акустических (речевых) сигналов путем приема и детектирования побочных электромагнитных излучений (на частотах работы высокочастотных генераторов ТСПИ и ВТСС), модулированных информационным сигналом: 1 – пользователь технического средства, имеющего акустоэлектрически незащищенный ВЧ-генератор, своей речью модулирует ПЭМИ ВЧ-генератора; 2 – разведчик в соседнем помещении (доме) принимает ПЭМИ ВЧ-генератора и выделяет речевой сигнал пользователя ТС; 3 – разведчик в транспортном средстве принимает ПЭМИ ВЧ-генератора и выделяет речевой сигнал пользователя ТС

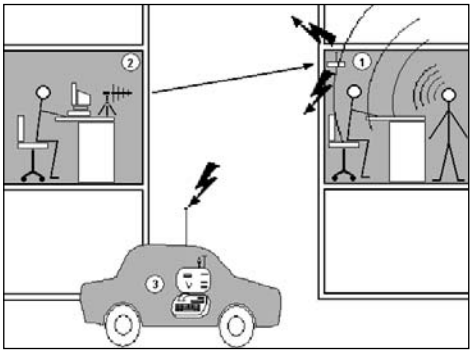

Рис. 22. Перехват акустических (речевых) сигналов путем «высокочастотного облучения» полуактивных закладных устройств: 1 – в помещении, «оснащенном» полуактивным закладным устройством, происходит обмен речевой информацией; 2 – разведчик облучает полуактивное закладное устройство мощным высокочастотным сигналом; 3 – разведчик в транспортном средстве принимает переизлученный закладным устройством ВЧ-сигнал, модулированный информацией речевого обмена в помещении

При облучении мощным высокочастотным сигналом помещения, в котором установлено такое закладное устройство, в последнем при взаимодействии облучающего электромагнитного поля со специальными элементами закладки (например, четвертьволновым вибратором) происходит образование вторичных радиоволн, т. е. переизлучение электромагнитного поля. Специальное устройство в закладке (например объемный резонатор) обеспечивает амплитудную, фазовую или частотную модуляцию переизлученного сигнала под воздействием акустической волны речевого сигнала. Подобного вида закладки иногда называют *полуактивными.*

Для перехвата информации по данному каналу кроме закладного устройства необходимы специальный передатчик с направленным излучением и приемник.

3.7. Каналы утечки речевой информации из объемов выделенных помещений

На рис. 23 представлены основные варианты возможной утечки речевой информации из объемов выделенных помещений. Все их можно объединить в две группы – это *акустические* каналы (обозначены буквами *а*, *б*, *в*), по которым информация может быть перехвачена с помощью микрофонов воздушной проводимости или прослушана непосредственно человеком, и *виброакустические* каналы (обозначены буквами *г*, *д*, *е*), по которым информация может быть зафиксирована с помощью микрофонов твердой среды (виброметров, велосиметров, акселерометров).

Наибольшую опасность представляют технологические окна и каналы с большой площадью поперечного сечения, такие как короба коммуникаций и воздуховоды вентиляции. Эти объекты являются по сути акустическими волноводами, и звуковые колебания могут распространяться по ним на значительные расстояния. Так, если поперечные размеры короба сравнимы с длиной звуковых волн $L = \lambda$, затухание при распространении по нему звука составляет $\delta = 0{,}01...1$ дБ/м и зависит от размеров короба, материала стенок и пр.

Следующими по степени опасности являются звуководы с размерами значительно меньше длины звуковых волн $L << \lambda$. Таковыми могут быть отверстия электропроводки, щели и трещины в строительных конструкциях, неплотности дверных и оконных проемов. Затухание звука в таких каналах весьма значительно $\delta = 1 ...20$ дБ/м.

Оно определяется вязкостью воздуха и зависит от поперечных размеров отверстий, шероховатости поверхности и продольной конфигурации отверстия.

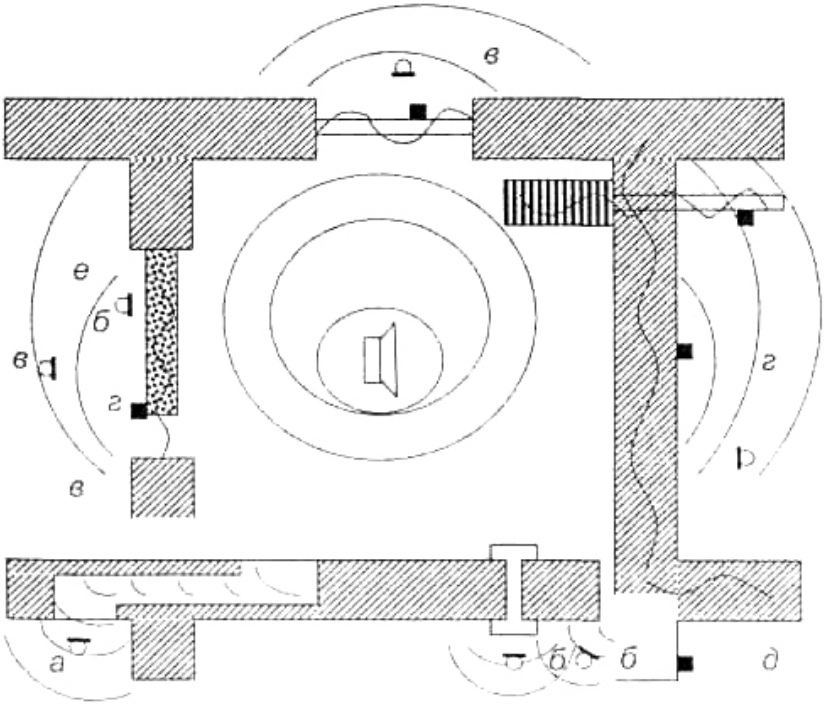

Рис. 23. Основные варианты возможной утечки речевой информации из объемов выделенных помещений

Несмотря на заметную величину затухания этого абсолютно недостаточно для обеспечения защиты информации. Так, если в стене толщиной 0,5 м имеется трещина с площадью поперечного сечения 5 мм^2 и длиной 0,75 м, звукоизоляция в области выхода этой трещины на поверхность будет составлять 18 дБ, в то время как при отсутствии трещины такая стена может обеспечить звукоизоляцию более 65 дБ.

Звуковые колебания могут распространяться за пределы выделенного помещения не только за счет тех или иных воздушных каналов, но и за счет переизлучения колебаний ограждающими строительными конструкциями.

Переизлучение звука за пределы выделенного помещения происходит за счет колебаний строительных конструкций, вызванных падающими на них звуковыми волнами. Так как толщина подавляющего большинства строительных конструкций (стены, полы, потолки, двери, окна) значительно меньше их поперечных размеров, процессы, происходящие в них, хорошо описываются теорией колебания мембран и пластин.

Основные практические выводы, вытекающие из данных положений:

– акустическое сопротивление ограждающих строительных конструкций в направлении, перпендикулярном их поверхности невелико;

– строительные конструкции имеют большое количество собственных мод колебаний.

Последнее явление в строительной акустике носит название «волнового совпадения». Оно возникает, когда длина падающей звуковой волны совпадает с длиной изгибной волны в строительной конструкции и приводит к значительному снижению звукоизоляции. Это проиллюстрировано рис. 24.

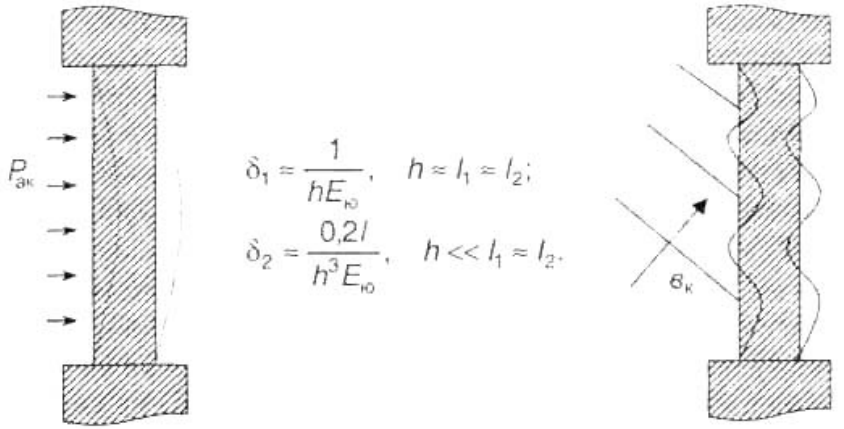

Рис. 24. Снижение звукоизоляции строительной конструкции

Так как за счет многократных переотражений звуковой волны в помещении равновероятны любые углы падений, возбуждаются все собственные моды колебаний строительных конструкций, что приводит к существенному снижению звукоизоляции.

При утечке акустических сигналов через вентиляционные воздухопроводы они ослабевают из-за изменения сечения, поглощений в изгибах воздуховодов. Затухание в прямых металлических воздуховодах составляет 0,15 дБ/м, в неметаллических – 0,2 – 0,3 дБ/м. При изгибах затухание достигает 3 – 7 дБ (на один изгиб), при изменениях сечения – 1 – 3 дБ. Ослабление сигнала на выходе из воздуховода помещения составляет 10 – 16 дБ.

3.8. Составные каналы утечки информации

Поиски путей повышения дальности добывания речевой информации привели к появлению составных каналов утечки информации. Применяются два вида последних: акусторадиоэлектронный и акустооптический.

Акусторадиоэлектронный канал утечки информации состоит из двух последовательно сопряженных каналов: акустического и радиоэлектронного. Приемником акустического канала является функциональный или случайно образованный акустоэлектрический преобразователь. Электрический сигнал с его выхода поступает на вход радиоэлектронного канала утечки информации – источника электрических или радиосигналов.

Структура акусторадиоэлектронного канала утечки информации приведена на рис. 25.

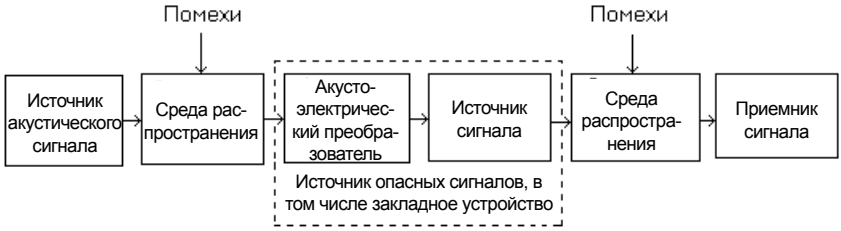

Рис. 25. Структура акусторадиоэлектронного канала утечки информации

Пара «акустоэлектрический преобразователь – источник сигнала» образует источник опасных сигналов или реализуется в закладном устройстве, размещаемом злоумышленником в помещении с конфиденциальной информацией. Закладные устройства создаются специально для подслушивания речевой информации и обеспечи-

вают повышение дальности составного акустического канала до единиц км и возможность съема информации злоумышленником за пределами контролируемой зоны.

Закладное устройство как ретранслятор является более надежным элементом канала утечки, чем источник опасного сигнала, так как процесс образования канала утечки информации на основе закладки управляем злоумышленником.

Другой способ повышения дальности акустического канала утечки информации реализуется путем создания составного акустооптического канала утечки информации. Схема его указана на рис. 26.

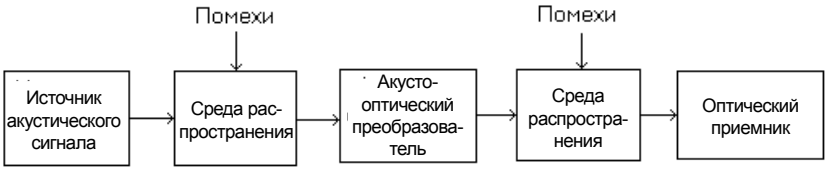

Рис. 26. Структурная схема акустооптического канала утечки информации

Составной акустооптический канал утечки информации образуется путем съема информации с плоской поверхности, колеблющейся под действием акустической волны с информацией, лазерным лучем в ИК-диапазоне. В качестве такой поверхности используется внешнее стекло закрытого окна в помещении, в которой циркулирует секретная (конфиденциальная) информация. Теоретически рассматривается возможность съема информации с внешней стороны стены помещения, но данных о реализации подобной идеи нет.

С целью образования оптического канала стекло облучается лазерным лучем с внешней стороны, например из окна противоположного дома. Луч лазера в ИК-диапазоне для посторонних лиц и находящихся в помещении невидим. В месте соприкосновения лазерного луча со стеклом происходит акустооптическое преобразование, т. е. модуляция лазерного луча акустическими сигналами от разговаривающих в помещении людей. Модулированный лазерный луч принимается оптическим приемником аппаратуры лазерного подслушивания, преобразуется в электрический сигнал, который усиливается, фильтруется, демодулируется и подается в головные телефоны для прослушивания оператором или в аудимагнитофон для консервации полученной информации.

Глава 4. КЛАССИФИКАЦИЯ И ХАРАКТЕРИСТИКА ТЕХНИЧЕСКИХ КАНАЛОВ ПЕРЕХВАТА ИНФОРМАЦИИ ПРИ ЕЕ ПЕРЕДАЧЕ ПО КАНАЛАМ СВЯЗИ

4.1. Общие положения

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

При перехвате решаются следующие основные задачи:

– поиск в пространстве и по частоте сигналов с нужной информацией;

– обнаружение и выделение сигналов, интересующих органы добывания;

– усиление сигналов и съем с них информации;

– анализ технических характеристик принимаемых сигналов;

– определение местонахождения (координат) источников представляющих интерес сигналов;

– обработка полученных данных с целью формирования первичных признаков источников излучения или текста перехваченного сообщения.

В настоящее время для передачи информации используют в основном КВ, УКВ, радиорелейные, тропосферные и космические каналы связи, а также кабельные и волоконно-оптические линии связи. В зависимости от вида каналов связи технические каналы перехвата информации можно разделить на электромагнитные, электрические и индукционные (рис. 27).

Рис. 27. Классификация технических каналов перехвата информации, передаваемой по каналам связи

4.2. Электромагнитный канал перехвата информации

Высокочастотные электромагнитные излучения передатчиков средств связи, модулированные информационным сигналом, могут перехватываться портативными средствами радиоразведки и при необходимости передаваться в центр обработки для их раскодирования (рис. 28).

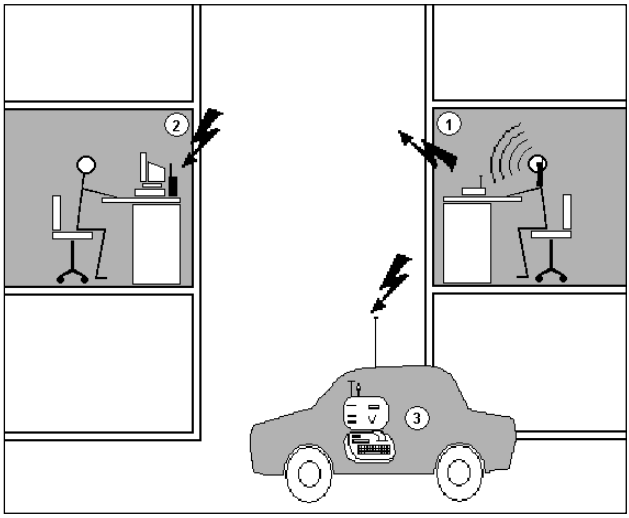

Рис. 28. Перехват информации, передаваемой по каналам радиосвязи: 1 – пользователь радиотелефона ведет по нему переговоры; 2 – разведчик в соседнем помещении (доме) принимает и прослушивает радиотелефонные переговоры пользователя; 3 – разведчик в транспортном средстве принимает и прослушивает радиотелефонные переговоры пользователя

Упрощенная структура типового комплекса средств перехвата приведена на рис. 29.

Типовой комплекс включает в себя: приемные антенны, радиоприемник, анализатор технических характеристик сигналов, радиопеленгатор, регистрирующее устройство.

Антенна предназначена для пространственной селекции и преобразования электромагнитной волны в электрические сигналы, амплитуда, частота и фаза которых соответствуют аналогичным характеристикам электромагнитной волны.

Радиоприемник служит для поиска и селекции радиосигналов по частоте, усиления и демодуляции (детектирования) выделенных сигналов, усиления и обработки демодулированных (первичных) сигналов: речевых, цифровых данных, видеосигналов и т. д.

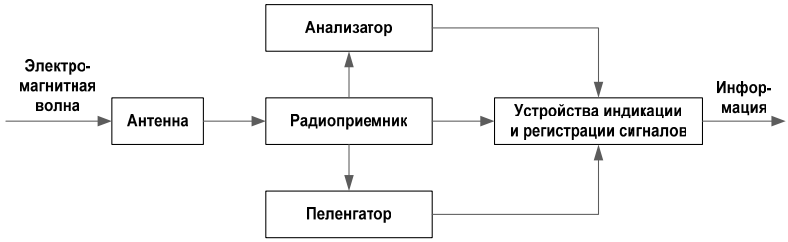

Рис. 29. Структура комплекса средств перехвата радиосигналов

Для анализа радиосигналов после частотной селекции и усиления они подаются на входы измерительной аппаратуры *анализатора*, определяющей параметры сигналов: частотные, временные, энергетические, виды модуляции, структуру кодов и др.

Радиопеленгатор предназначен для определения направления на источник излучения (пеленг) или его координат.

Регистрирующее устройство обеспечивает запись сигналов для документирования и последующей обработки.

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

4.3. Электрический канал перехвата информации

Электрический канал перехвата информации, передаваемой по кабельным линиям связи, предполагает контактное подключение аппаратуры перехвата к кабельным линиям связи (рис. 30).

Подключение средства перехвата электрических сигналов к электрическим проводам кабеля может быть последовательным (рис. 31, *а*) или параллельным (рис. 31, *б*).

При последовательном подключении в разрыв провода линии включается элемент приемника перехвата – сопротивление, сигнал с которого усиливается и воспроизводится в форме, доступной для

человека, анализа или записи на аудио- или видеомагнитофон. При параллельном способе средство перехвата подключается к проводам линии параллельно.

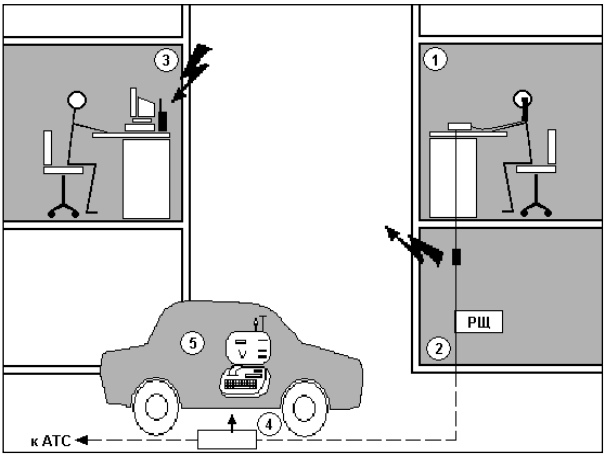

Рис. 30. Съем информации с проводных (кабельных) линий связи: 1 – сотрудник по телефону АТС обменивается конфиденциальной информацией; 2 – к телефонной линии подключено закладное устройство с микрорадиопередатчиком; 3 – разведчик в соседнем помещении (доме) принимает радиосигнал от телефонной закладки; 4 – над кабельной линией установлено устройство индукционного съема информации; 5 – в транспортном средстве происходит прием сигнала от индукционного устройства съема информации

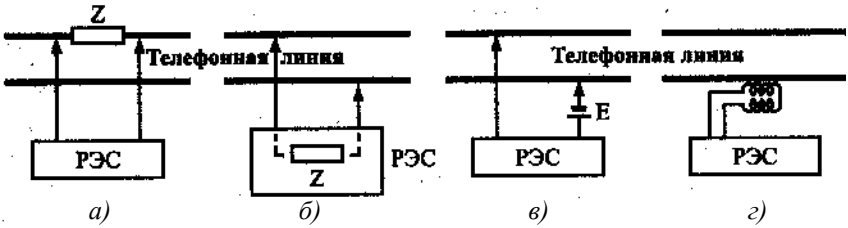

Рис. 31. Варианты подключения средств подслушивания (РЭС) к телефонной линии

Наиболее простым средством перехвата сигнала с целью подслушивания речевой информации в телефонных линиях связи является телефонная трубка, которая подключается к проводам со снятой изоляцией телефонной линии с помощью контактов типа «крокодил».

Последовательно или параллельно подключаемое средство перехвата можно представить в виде эквивалентного комплексного (активного и реактивного) сопротивления *Z*. Поэтому контактное подключение уменьшает энергию сигнала и изменяет электрические параметры линии, к которой подключено средство перехвата. Эти изменения представляют собой демаскирующие признаки средства перехвата, по которым оно может быть обнаружено. Вероятность обнаружения зависит от величины изменения параметров линии и их стабильности. Поэтому средства перехвата подключаются к линии связи или через согласующее устройство, незначительно снижающее падение напряжения, или через специальное устройство 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.

Для снижения влияния подключенного средства перехвата уменьшают величину включенного последовательно сопротивления до единиц Ома или увеличивают входное сопротивление параллельно подключаемого средства до единиц МОма. Уменьшение напряжения в линии можно компенсировать подачей внешнего дополнительного напряжения *E* противоположного знака, как показано на рис. 31, *в*.

Современные средства защиты информации в проводных линиях позволяют обнаруживать последовательно включаемые средства с сопротивлением до 5 Ом и параллельно подключаемые – до 5 МОм.

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. Устройства, подключаемые к телефонным линиям связи и совмещенные с устройствами передачи информации по радиоканалу, обычно называют телефонными закладками.

4.4. Индукционный канал перехвата информации

В случае применения сигнальных устройств контроля целостности линии связи и ее активного и реактивного сопротивления, факт контактного подключения к ней аппаратуры разведки будет обнаружен. Поэтому спецслужбы наиболее часто используют индукционный канал перехвата информации, не требующий 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 (см. рис. 29).

Бесконтактные средства подключения (датчики) перехватывают сигналы, которые излучают провода при протекании по ним электрического тока. В этом случае средства перехвата не отбирают у сигналов энергию и обнаруживаются существенно хуже, только по изменению индуктивности и емкости линии за счёт своих индуктивности и емкости, а также по изменению волнового сопротивления линии. Вариант подключения бесконтактного дифференциального индуктивного датчика показан на рис. 31, *г*. В катушках датчика наводят ЭДС как полей, излучаемых токами в проводниках линии, так и других внешних полей. С целью компенсации одинаковых по уровню ЭДС внешних полей катушки включены встречно. За счет большей близости одной из катушек к проводу линии наводимая в ней ЭДС больше по величине, чем в более удаленной от провода катушке.

Итак, индукционные датчики применяются в основном для съема информации с симметричных высокочастотных кабелей. Современные индукционные датчики способны регистрировать информацию с кабелей, защищенных не только изоляцией, но и двойной броней из стальной ленты и стальной проволоки, плотно обвивающей кабель. Для бесконтактного съема информации с незащищенных телефонных линий связи могут использоваться специальные высокочувствительные низкочастотные усилители, снабженные магнитными антеннами. Некоторые средства бесконтактного съема информации могут совмещаться с радиопередатчиками для передачи ее на контрольный пункт перехвата.

4.5. Перехват информации из линий опто-волоконной связи

С разработкой волоконно-оптической технологии появились направляющие линии связи в оптическом диапазоне, которые в силу их преимуществ по сравнению с традиционными электрическими проводниками рассматриваются как более совершенная физическая среда для передачи больших объемов информации.

Хотя возможность утечки информации из волоконно-оптического кабеля существенно ниже, чем из электрического, при определенных условиях такая утечка реальна. Для съема информации теоретически можно разрушить защитную оболочку кабеля, найти нужное оптическое волокно, прижать фотодетектор приемника к очищенной площадке волокна и изогнуть волокно на угол, при котором не обеспечивается полное отражение оптического луча внутри волокна и часть световой энергии попадает на фотодетектор приемника. Практически информацию из оптического волокна добывают в местах соединения кабеля с техническими средствами или участков кабеля друг с другом. Во-первых, в местах соединения трудно исключить излучение света в окружающее пространство из-за смещения соединяемых волокон, наличия зазора между ними, непараллельности торцевых поверхностей волокон, углового рассогласования осей волокон и различия в их диаметрах. Во-вторых, в этих местах реален доступ к волоконно-оптическому кабелю и оперативная замена штатных коннекторов на коннекторы с отводом части световой энергии к фотодетектору оптического приемника злоумышленника.

Итак, перехват опто-волоконных сигналов возможен в двух вариантах:

– в местах входа (выхода) оптических сигналов в (из) кабеля;

– при деформации оптического кабеля, при которой угол его изгиба превышает угол предельного отражения лучей света в кабеле.

Глава 5. ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ВИДОВОЙ ИНФОРМАЦИИ

5.1. Общие сведения

Наряду с информацией, обрабатываемой в ТСПИ, и речевой информацией важную роль играет видовая (оптическая) информация, получаемая техническими средствами перехвата в виде изображений объектов или документов.

В зависимости от характера информации можно выделить следующие способы ее получения:

– наблюдение за объектами;

– съемка объектов;

– съемка (снятие копий) документов.

Классификация способов скрытого видеонаблюдения и съемки приведена на рис. 32. Структура оптического канала утечки информации имеет вид, показанный на рис. 33.

В общем случае источником оптического сигнала является объект наблюдения, который излучает сигнал или переотражает свет другого, внешнего источника. Отражательная способность объектов наблюдения зависит от длины волны падающего света и спектральных характеристик поверхности объекта наблюдения. Отражательная способность ряда природных фонов (травы, листвы и др.) и биологических объектов возрастает в несколько раз при смещении длины волны падающего света в область более длинных волн, а для неживых объектов она меняется мало в широком диапазоне длин волн.

Основным и наиболее мощным внешним источником света, освещающим объекты наблюдения в дневное время, является Солнце. При температуре поверхности около 6000 °С Солнце излучает огромное количество энергии в достаточно широкой полосе – от ультрафиолетового до инфракрасного (0,17 – 4 мкм). Максимум солнечного излучения приходится на 0,47 мкм, в ультрафиолетовой части оно резко убывает, в инфракрасной области зависимость уровня излучения от длины волны регистрируется в виде широкой и пологой кривой.

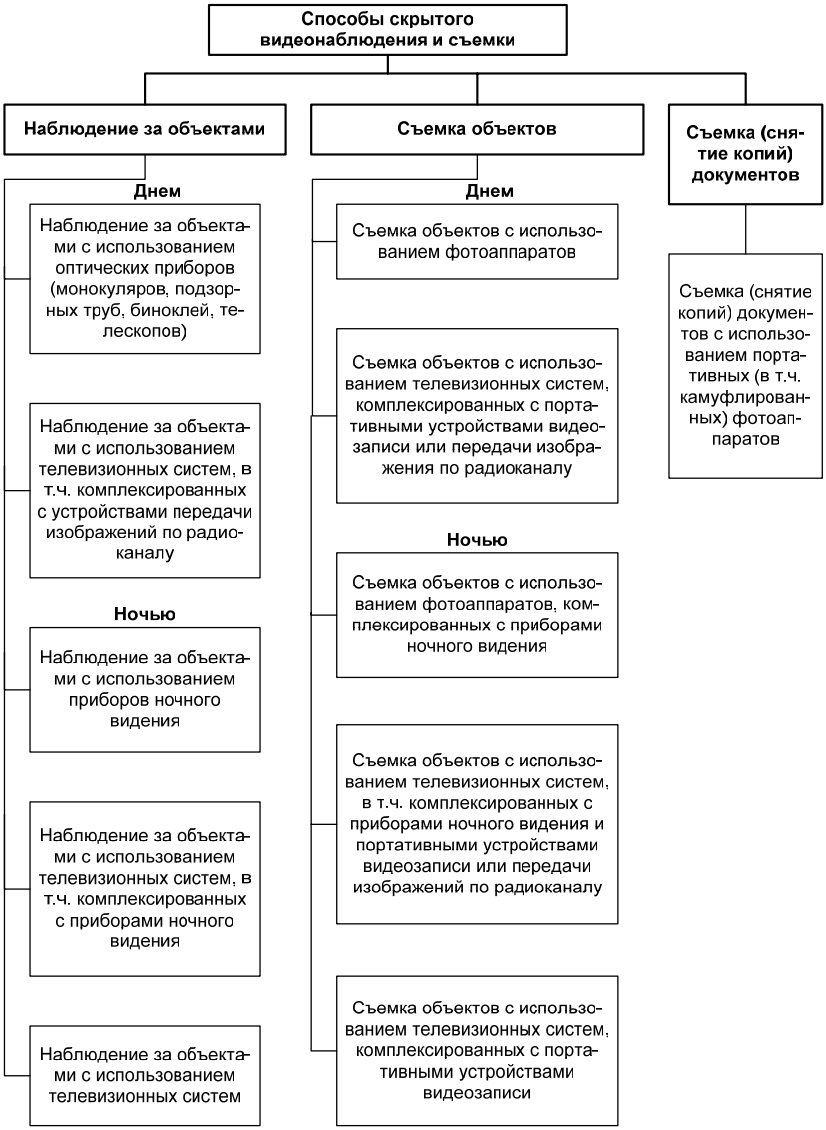

Рис. 32. Классификация способов скрытого видеонаблюдения и съемки

Освещенность в дневное время земной поверхности Солнцем составляет в зависимости от его высоты, облачности атмосферы 10^1 – 10^5 лк. С движением Солнца к горизонту Земли, когда зенитное расстояние между ними достигает максимума, освещенность Солнцем уменьшается до 10 лк. При этом изменяется спектр солнечного света. Так как при прохождении толщи атмосферы синие и фиолетовые лучи ослабляются сильнее, чем оранжевые и красные, максимум излучения Солнца смещается в красную область цвета. С заходом Солнца за горизонт и наступлением сумерек освещенность убывает вплоть до наступления астрономических сумерек, за которыми следует наиболее темное время суток – ночь.

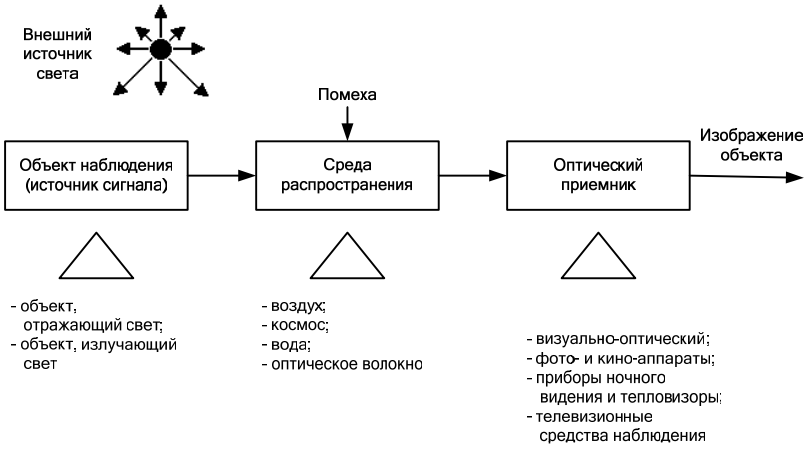

Рис. 33. Структура оптического канала утечки информации

Освещенность в лунную ночь при безоблачном небе, когда так называемую *естественную ночную освещенность (ЕНО)* создает отраженный от Луны солнечный свет, составляет около 0,3 лк. Величина ЕНО света Луны в течение месяца меняется приблизительно в 100 раз в зависимости от взаимного положения Луны, Солнца и Земли. Лунный месяц разделяется по уровню освещенности на четыре части, каждая длительностью около недели.

Источниками излучения в безлунную ночь при безоблачном небе, называемого *звездным светом*, являются солнечный свет, отраженный от планет и туманностей, свет звезд, а также свечение кислорода и азота в верхних слоях атмосферы на высоте 100 – 300 км. Освещенность поверхности Земли звездным светом составляет в среднем 0,001 лк.

В инфракрасном диапазоне мощность излучения объекта зависит от температуры тела или его элементов, мощности падающего на объект света и коэффициента отражения объекта в этом диапазоне. Коэффициент теплового излучения для реальных объектов непостоянен по спектру и определяется в соответствии с законом Кирхгофа отношением спектральной плотности энергетической яркости объекта к спектральной плотности энергетической яркости абсолютно черного тела, которое обладает максимумом энергии теплового излучения по сравнению со всеми другими источниками при той же температуре.

Объекты могут иметь собственные источники тепловой энергии, например, высокотемпературные элементы машин, дизельэлектростанции и другие, температура которых значительно выше температуры фона. Максимум теплового излучения таких объектов смещается в коротковолновую область, что является их демаскирующим признаком.

Среду распространения в оптическом канале утечки информации образуют:

– безвоздушное (космическое) пространство;
– атмосфера;
– вода;
– оптические волокна.

В общем случае потенциальные оптические каналы утечки информации имеют достаточно устойчивые признаки. Типовые варианты оптических каналов утечки информации приведены в табл. 1.

Таблица 1

Объект наблюдения (источник оптического сигнала)	Среда распространения	Оптический приемник
Документ, продукция в помещении	Воздух Воздух + стекло окна	Глаза человека + бинокль, фотоаппарат
Продукция во дворе, в машине, на платформе	Воздух Атмосфера + безвоздушное пространство	Глаза человека + бинокль, фотоаппарат Фото-, ИК-, телевизионная аппаратура на КА
Человек в помещении, во дворе, на улице	Воздух Воздух + стекло	Глаза человека + бинокль, фото-, кино-, телевизионная аппаратура

В качестве *оптических приемников* оптических каналов утечки информации используются:

– оптические приборы, расширяющие возможности зрения наблюдателя (бинокли, зрительные трубы, специальные телескопы и др.);

– фото- и киноаппараты, видеокамеры, консервирующие наблюдаемое изображение;

– телевизионные камеры, позволяющие передавать движущееся изображение на сколь угодно большое расстояние;

– приборы ночного видения, преобразующие невидимое глазом инфракрасное изображение в видимое;

– тепловизоры, позволяющие наблюдать объект в свете его собственного теплового излучения.

5.2. Наблюдение за объектами

В зависимости от условий наблюдения и освещения для наблюдения за объектами могут использоваться различные технические средства: днем – оптические приборы (монокуляры, подзорные трубы, бинокли, телескопы и т. д.), телевизионные камеры; ночью – приборы ночного видения, телевизионные камеры, тепловизоры.

Так как физическая природа носителя информации в видимом и инфракрасном диапазонах одинакова, то различные средства наблюдения, применяемые для добывания информации в этом диапазоне, имеют достаточно общую структуру. Ее можно представить в виде, приведенном на рис. 34.

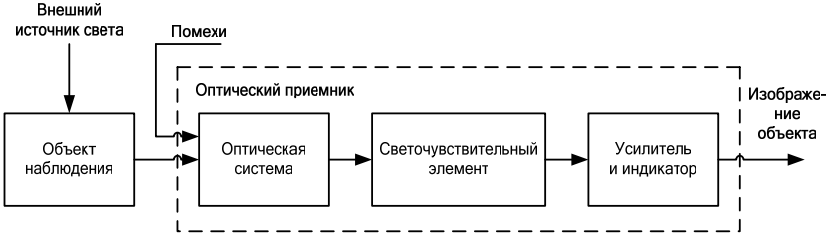

Рис. 34. Структурная схема оптического приемника

Большинство средств наблюдения представляют собой оптический приемник, содержащий оптическую систему, светоэлектри-

ческий элемент, усилитель и индикатор. В зависимости от вида светочувствительного элемента оптические приборы делят на визуально-оптические, фотографические и оптико-электронные. В визуально-оптических средствах наблюдения светочувствительным элементом является сетчатка глаза человека, в традиционных фото- и киноаппаратах – фотопленка, а в оптико-электронных приборах – мишень светоэлектрического преобразователя (СЭП).

На рис. 35 представлен вариант технологии визуального наблюдения и съемки удаленного изображения.

Для наблюдения с большого расстояния используются средства с длиннофокусными оптическими системами, а при наблюдении с близкого расстояния – камуфлированные скрытно установленные телевизионные камеры. При этом изображение с телевизионных камер может передаваться на мониторы как по кабелю, так и по радиоканалу.

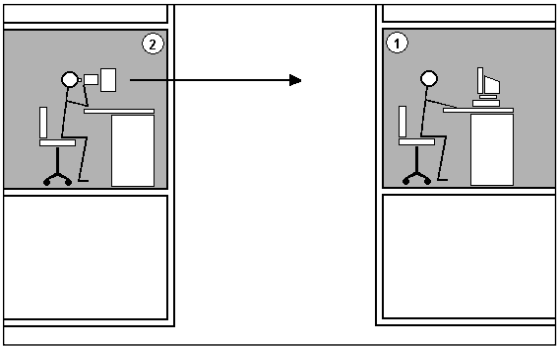

Рис. 35. Визуальное наблюдение и съемка объектов с использованием фотографических и телевизионных систем: 1 – пользователь незащищенной от видеонаблюдения ПЭВМ вызывает на экран монитора информацию; 2 – разведчик в соседнем доме осуществляет визуальнооптическое наблюдение, фотографирование и видеосъемку информации на экране монитора пользователя

5.3. Съемка объектов

Съемка объектов проводится для документирования результатов наблюдения и более подробного изучения объектов. Для съемки объектов используются телевизионные и фотографические средства.

При съемке объектов, так же как и при наблюдении за ними, использование тех или иных технических средств обусловлено условиями съемки и временем суток. Для съемки объектов днем с большого расстояния используются фотоаппараты и телевизионные камеры с длиннофокусными объективами или совмещенные с телескопами.

Для съемки объектов днем с близкого расстояния применяются портативные камуфлированные фотоаппараты и телекамеры, совмещенные с устройствами видеозаписи или передачи изображений по радиоканалу.

Вариант технологии скрытой съемки с передачей изображения по радиоканалу приведен на рис. 36.

Съемка объектов ночью проводится, как правило, с близкого расстояния. Для этих целей используются портативные фотоаппараты и телевизионные камеры, совмещенные с приборами ночного

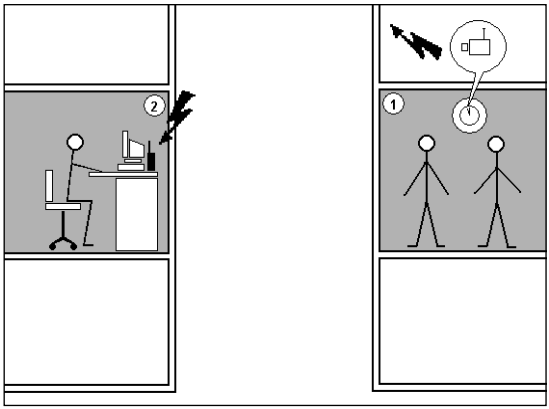

Рис. 36. Скрытая съемка объектов с использованием портативных телевизионных систем, комплексированных с устройствами передачи изображений по радиоканалу: 1 – в помещении, «оснащенном» настенными часами с портативной телевизионной камерой и устройством передачи видео- и аудиосигналов по радиоканалу, происходит обмен конфиденциальной информацией; 2 – разведчик в соседнем помещении (доме) принимает видео- и аудиосигналы от скрытно установленной телекамеры

видения, или тепловизоры, а также портативные закамуфлированные телевизионные камеры высокой чувствительности, совмещенные с устройствами передачи информации по радиоканалу.

Съемка документов осуществляется, как правило, с использованием портативных фотоаппаратов.

Глава 6. МАТЕРИАЛЬНО-ВЕЩЕСТВЕННЫЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ

6.1. Общие положения

Особенность этого канала вызвана спецификой источников и носителей информации по сравнению с другими каналами. Источниками и носителями информации в нем являются субъекты (люди) и материальные объекты (макро- и микрочастицы), которые имеют четкие пространственные границы локализации, за исключением излучений радиоактивных веществ. Утечка информации в этих каналах сопровождается физическим перемещением людей и материальных тел с информацией за пределами контролируемой зоны. Для более четкого описания рассматриваемого канала целесообразно уточнить состав источников и носителей информации.

Основные источники материально-вещественного канала утечки информации:

– черновики различных документов и макеты материалов, узлов, блоков, устройств, разрабатываемых в ходе научно-исследовательских и опытно-конструкторских работ, ведущихся на предприятии (организации); отходы делопроизводства и издательской деятельности на предприятии (организации), в том числе использованная копировальная бумага, забракованные листы при оформлении документов и их размножении;

– нечитаемые дискеты ПЭВМ из-за их физических дефектов и искажений загрузочных или других кодов;

– бракованная продукция и ее элементы;

– отходы производства в газообразном, жидком и твердом виде;

– радиоактивные материалы.

Перенос информации в этом канале за пределы контролируемой зоны возможен следующими субъектами и объектами:

– сотрудниками организации и предприятия;

– воздушными массами атмосферы;

– жидкой средой;

– излучениями радиоактивных веществ.

Эти носители могут переносить все виды информации: семантическую и признаковую, а также демаскирующие вещества.

Семантическая информация содержится в черновиках документов, схем, чертежей; информация о видовых и сигнальных демаскирующих признаках – в бракованных узлах и деталях, в характеристиках радиоактивных излучений и т. д.; демаскирующие вещества – в газообразных, жидких и твердых отходах производства.

6.2. Структура материально-вещественного канала утечки информации

Структура материально-вещественного канала утечки информации приведена на рис. 37.

Рис. 37. Структура материально-вещественного канала утечки информации

Приемники информации этого канала достаточно разнообразны. Это эксперты зарубежной разведки или конкурента, средства для физического и химического анализа, средства вычислительной техники, приемники радиоактивных излучений и др.

Потери носителей с ценной информацией возможны при отсутствии на предприятии четкой системы учета носителей с закрытой информацией. Например, испорченный машинисткой лист отчета может быть выброшен ею в корзину для бумаги, из которой он будет уборщицей перенесен в бак для мусора на территории предприятия, а далее при перегрузке бака или транспортировки мусора на свалку лист может быть унесен ветром и поднят прохожим. Конечно, вероятность обеспечения случайного контакта с этим листом злоумышленника невелика, но если последний активно занимается добыванием информации, то область пространства, в котором возможен контакт, значительно сужается и вероятность утечки повышается.

Для предприятий химической, парфюмерной, фармацевтической и других сфер разработки и производства продукции, техноло-

гические процессы которых сопровождаются использованием или получением различных газообразных или жидких веществ (материалов), возможно образование каналов утечки информации через выбросы в атмосферу газообразных или слив в водоемы жидких демаскирующих веществ.

Подобные каналы образуются при появлении возможности добывания демаскирующих веществ в результате взятия злоумышленниками проб воздуха, воды, земли, снега, пыли на листьях кустарников и деревьев, траве и цветах в окрестностях предприятия (организации).

В зависимости от розы (направлений) и скорости ветра демаскирующие вещества в газообразном виде или в виде взвешенных твердых частиц могут распространяться на расстояние в единицы и десятки км, достаточное для безопасного взятия проб злоумышленниками. Аналогичное положение наблюдается и для жидких отходов.

Конечно, концентрация демаскирующих веществ при удалении от источника убывает, но при утечке их в течение некоторого времени она может превышать допустимые значения за счет накопления демаскирующих веществ в земле, растительности и подводной флоре и фауне.

Отходы могут продаваться другим предприятиям для использования в производстве иной продукции, очищаться перед сливом в водоемы, уничтожаться или подвергаться захоронению на время саморазрушения или распада. Последние операции выполняются для высокотоксичных веществ, утилизация которых другими способами экономически нецелесообразна, и для радиоактивных отходов, которые нельзя нейтрализовать физическими или химическими способами.

Утечка информации о радиоактивных веществах возможна в результате выноса радиоактивных веществ сотрудниками предприятия (организации) или регистрации злоумышленником их излучений с помощью соответствующих приборов

Дальность канала утечки информации о радиоактивных веществах через их излучения невелика: для α-излучений она составляет в воздухе единицы миллиметров, β-излучений – сантиметров, и только γ-излучения можно регистрировать на удалении в сотни метров от источника излучения.

Глава 7. КОМПЛЕКСИРОВАНИЕ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

7.1. Общие положения

Многообразие рассмотренных каналов утечки информации предоставляет злоумышленнику большой выбор возможностей для добывания информации. Из анализа возможностей каждого из рассмотренных каналов можно сделать следующие выводы:

1. Утечка семантической информации возможна по всем техническим каналам. По возможностям, а следовательно, по угрозе безопасности информации они ранжируются в такой последовательности: радиоэлектронный, акустический и оптический. Однако в конкретных условиях возможны иные ранги каналов, например, когда имеется реальная возможность прослушивания совещаний или фотографирования документов.

2. Наибольшими потенциальными возможностями по добыванию информации о видовых демаскирующих признаках обладает оптический канал, в котором информация добывается путем фотографирования. Это обусловлено особенностями фотоизображения, которое:

– имеет самое высокое разрешение; даже на относительно большом расстоянии в сотни километров от объекта наблюдения разрешение при космической фотосъемке достигает 15 – 30 см на местности;

– имеет самую высокую информационную емкость, обусловленную максимумом демаскирующих признаков, в том числе наличием такого информативного признака, как цвет;

– обеспечивает относительно низкий уровень геометрических искажений.

Информационные емкости телевизионных изображений примерно на порядок ниже фотоизображений. Телевизионные изображения имеют более низкий уровень разрешения, повышенный уровень яркостных искажений за счет неравномерности спектраль-

но-яркостных характеристик фотокатода передающих телевизионных трубок или приборов с зарядовой связью, повышенный уровень геометрических искажений за счет дополнительных искажений при формировании электронного растра.

Изображения в ИК-диапазоне обладают еще более низкими информационными параметрами. Кроме более низкой разрешающей способности и больших искажений для изображений в ИК-области характерны крайняя изменчивость в течение суток. Однако, как уже отмечалось при рассмотрении каналов утечки информации, изображение в каждом из них содержит дополнительные признаки за счет различной их природы.

3. Основным каналом получения сигнальных демаскирующих признаков является радиоэлектронный. В значительно меньшем объеме утечка информации о сигнальных демаскирующих признаках возможна в акустическом и материально-вещественном каналах.

Для добывания информации злоумышленник, как правило, использует несколько каналов ее утечки. Комплексирование последних основывается на следующих принципах:

– комплексируемые каналы дополняют друг друга по своим возможностям;

– эффективность комлексирования повышается при уменьшении зависимости между источниками информации и демаскирующими признаками в разных каналах.

Комплексирование каналов утечки информации обеспечивает:

– увеличение вероятности обнаружения и распознавания объектов за счет расширения их текущих признаковых структур;

– повышение достоверности семантической информации и точности измерения признаков, в особенности в случае добывания информации из недостаточно надежных источников.

Когда возникают сомнения в достоверности информации, то с целью исключения дезинформации, полученные сведения и данные перепроверяют по другому каналу.

7.2. Виды комплексирования

Возможны два основных вида комплексирования каналов утечки информации – обеспечение утечки информации от одного источника по нескольким параллельно функционирующим канала (рис. 38, *а*) и от разных источников (рис. 38, *б*).

В первом варианте одна и та же информация распространяется по различным направлениям одним или разными носителями. Например, речевая информация разговаривающих в помещении людей может быть подслушана через дверь или стену, снята с опасных сигналов или передана с помощью закладного устройства.

Так как вероятность воздействия помех в разных каналах на одинаковые элементы информации мала, то в этом случае повышается достоверность суммарной информации после обработки ее в соответствующем органе. При независимости помех в *n* каналах утечки информации вероятность поражения одного и того же элемента информации при комплексировании *n* каналов рассчитывается по формуле $Pn = \prod_{i=1}^{n} P_i$, где P_i – вероятность поражения элемента информации в *i*-м канале.

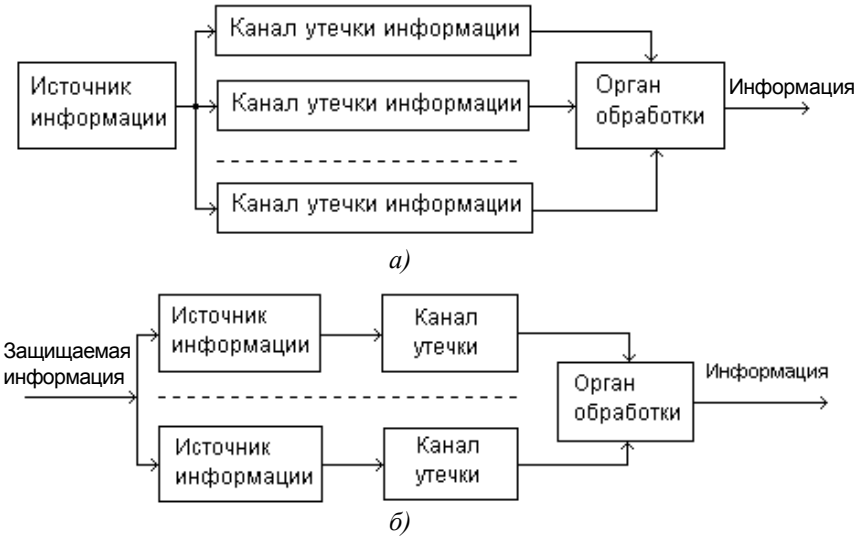

Рис. 38. Варианты комплексного использования каналов утечки

Однако если источник не владеет достоверной информацией или занимается дезинформацией, то рассмотренный вариант комплексирования не повышает достоверность итоговой информации.

Для обеспечения такой возможности одна и та же информация добывается от нескольких источников, например, из документа и от специалистов, участвующих в создании этой информации. При таком комплексировании двух каналов вероятность внедрения дезинформации можно оценить по формуле

$$P_{Д} = P_1 P_2 + r\sqrt{P_1(1-P_1)P_2(1-P_2)},$$

где P_1 и P_2 – значения вероятности появления дезинформации в 1-м и 2-м каналах; r – коэффициент корреляции между информацией в этих каналах.

Коэффициент r корреляции характеризует статистическую зависимость между информацией (содержанием или признаками) в каналах. При $r = 1$ по каналам производится утечка информации одинакового содержания или об одинаковых признаках с разными значениями, при $r = 0$ – источники независимые.

Как следует из вышеприведенной формулы, для уменьшения риска получения дезинформации необходимо снижать коэффициент корреляции между источниками информации.

КОНТРОЛЬНЫЕ ВОПРОСЫ И ЗАДАНИЯ

1. Дайте определение технического канала утечки информации.

2. Назовите характеристики и дайте классификацию каналов утечки.

3. В чем отличие основных от вспомогательных технических средств и систем?

4. Дайте определение контролируемой зоны.

5. Назовите основные виды каналов утечки информации, обрабатываемой ТСПИ.

6. Покажите, на каких физических процессах ОТСС и ВТСС построены основные виды каналов утечки с информационных носителей.

7. Объясните физическую сущность возникновения побочных электромагнитных излучений.

8. Какие причины приводят к возникновению электрических каналов утечки информации?

9. Назовите основные виды каналов утечки акустической информации.

10. Покажите, на каких физических процессах в помещениях и размещенных в них ОТСС и ВТСС построены основные виды утечки акустической информации из помещений.

11. Чем обусловлены каналы утечки речевой информации из объемов выделенных помещений?

12. Как создаются составные каналы утечки информации?

13. Приведите структуру комплекса средств перехвата радиосигналов.

14. Как реализуется метод «высокочастотного навязывания»?

15. На чем основана реализация лазерного канала утечки информации?

16. Как реализуется метод «высокочастотного облучения»?

17. Назовите основные виды каналов утечки информации, передаваемой по каналам связи.

18. Назовите способы получения видовой информации.

19. Какие излучения относятся к электромагнитным каналам утечки?

20. За счет чего возникают электрические каналы утечки информации?

21. Каким параметром определяется зона возможного перехвата информации?

22. Каковы основные акустические параметры речевых сигналов?

23. От чего зависит звукоизоляция основных строительных конструкций?

24. Что является наиболее распространенными причинами снижения звукоизоляции строительных конструкций?

25. Какие элементы строительных конструкций наиболее опасны с точки зрения несанкционированного съема информации?

26. Чем обусловлены материально-вещественные каналы утечки информации?

27. Чем и как обусловлено комплексирование каналов утечки информации?

ЗАКЛЮЧЕНИЕ

Источниками преднамеренных угроз утечки и безопасности информации могут быть органы зарубежной разведки, разведки коммерческих структур внутри государства, криминальные структуры, завербованные, психически больные или недовольные своим положением сотрудники организации. К источникам случайных угроз относятся стихийные силы, приведшие в негодное состояние элементы инфраструктуры мест работы средств информационного обеспечения, технические средства с неисправными элементами, программы с ошибками и вирусами, неквалифицированные или плохо выполняющие свои обязанности операторы и обслуживающий персонал, грызуны и насекомые в местах размещения радиоэлектронных средств. Источниками угроз утечки являются люди и источники сигналов.

Профессионально добывание информации осуществляют органы государственной и коммерческой разведки вероятного противника. Информацию с помощью технических средств добывает техническая разведка. Техническая разведка по виду носителя добываемой информации делится на акустическую, оптическую, радиоэлектронную, компьютерную, химическую, радиационную, магнитометрическую, сейсмическую.

Акустическая, оптическая и радиоэлектронная разведки состоят из многочисленных подвидов. Акустическая разведка по виду среды распространения акустической волны делится на воздушно-акустическую (акустическую), гидроакустическую и виброакустическую. Оптическая разведка включает визуально-оптическую, фотографическую, оптико-электронную (телевизионную, инфракрасную, лазерную). Радиоэлектронная разведка по виду добываемой информации разделяется на радио-, радиотехническую, радиолокационную,

радио-теплодокационную и разведку ПЭМИН. По виду носителя средств различают техническую разведку на наземную, воздушную, космическую и морскую.

Возможности добывания информации технической разведкой вероятного противника зависят от наличия у нее возможных способов доступа к источникам информации, в том числе с применением технических средств, обеспечивающих условия разведывательного контакта через выявленные ей или преднамеренно созданные технические каналы утечки информации. Следовательно, главная задача защиты информации техническими средствами – своевременно обнаружить, исключить и закрыть все естественные и искусственно созданные технические каналы вероятной утечки защищаемой информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК*

1. *Абалмазов, Э. И.* Новые технологии защиты телефонных переговоров / Э. И. Абалмазов // Специальная техника. – 1998. – № 1. – С. 4 – 8.

2. *Андрианов, В. И.* «Шпионские штучки» и устройства для защиты объектов и информации : справ. пособие / В. И. Андрианов, В. А. Бородин, А. В. Соколов. – СПб : Лань, 1996. – 272 с.

3. *Барсуков, В. С.* Безопасность: технологии, средства, услуги / В. С. Барсуков. – М. : КУДИЦ-ОБРАЗ, 2001. – 496 с.

4. *Вакин, С. А.* Основы радиопротиводействия и радиотехнической разведки / С. А. Вакин, Л. Н. Шустов. – М. : Сов. радио, 1968. – 448 с.

5. *Волобуев, С. В.* Оценка акустической защищенности без применения инструментальных средств / С. В. Волобуев // Системы безопасности связи и телекоммуникаций. – 1999. – № 25. – С. 38 – 45.

6. *Волгин, М. Л.* Паразитные связи и наводки / М. Л. Волгин. – М. : Сов. радио, 1965. – 232 с.

7. *Герасименко, В. А.* Основы защиты информации / В. А. Герасименко, А. А. Малюк. – М. : МИФИ, 1998. – 538 с.

8. ГОСТ РВ 50170-92. Противодействие ИТР. Термины и определения. – М. : Госстандарт России : Изд-во стандартов, 1992.

9. ГОСТ Р 50992-96. Защита информации. Термины и определения. – М. : Госстандарт России : Изд-во стандартов, 1996.

10. ГОСТ Р 50840-95. Методы оценки качества, разборчивости, узнаваемости. – М. : Госстандарт России.

11. *Заборов, В. И.* Звукоизоляция в жилых и общественных зданиях / В. И. Заборов, Э. М. Лалаев, В. К. Никольский. – М. : Стройиздат, 1979. – 154 с.

12. О государственной тайне : федер. закон от 21 июля 1998 г. № 5486-1. – 1998 г.

13. Об информации, информатизации и защите информации : федер. закон № 24-ФЗ-20.02 // Консультант+. – 1995.

14. *Калинин, С. В.* О некоторых новых тенденциях в развитии систем виброакустического зашумления / С. В. Калинин // Защита информации. «Конфидент». – 1999. – №4 – 5. – С. 74 – 79.

15. *Кравчук, П. Н.* Генерация и методы снижения шума и звуковой вибрации / П. Н. Кравчук. – М. : Изд-во МГУ, 1991. – 183 с.

* Печатается в авторской редакции.

16. *Маркоменко, В. И.* Защита информации в информационно-телекоммуникационных системах органов государственной власти / В. И. Маркоменко // Системы безопасности связи и телекоммуникаций. – 1997. – № 1. – С. 72 – 76.

17. *Мироничев, С.* Коммерческая разведка и контрразведка, или промышленный шпионаж в России и методы борьбы с ним / С. Мироничев. – М. : Дружок, 1995. – 223 с.

18. *Пятачков, А. Г.* Рекомендации по защите информации от утечки по техническим каналам на объектах информатизации / А. Г. Пятачков // Защита информации. «Конфидент». – 1999. – № 4 – 5. – С. 80 – 85.

19. Технические средства видовой разведки / под ред. А. А. Хорева. – М. : РВСН, 1997. – 327 с.

20. *Торокин, А. А.* Основы инженерно-технической защиты информации / А. А. Торокин. – М. : Ось-89, 1998. – 336 с.

21. *Халяпин, Д. Б.* Акустоэлектрические, акустопреобразовательные каналы утечки информации и возможные способы их подавления / Д. Б. Халяпин // Мир безопасности. – № 5, – С. 47 – 53.

22. *Он же.* Визуально-оптический канал утечки информации / Д. Б. Халяпин // Мир безопасности. – 1998. – № 7. – С. 48 – 50.

23. *Он же.* Стены и уши. Защита информации / Д. Б. Халяпин. – М. : Мир безопасности. – 1998. – С. 76 – 81.

24. *Он же.* Физические основы возникновения вибрационного (структурного) канала утечки информации и возможности его подавления / Д. Б. Халяпин // Мир безопасности. – 1999. – № 2. – С. 42 – 48.

25. *Халяпин, Д. Б.* Основы защиты промышленной и коммерческой информации : термины и определения / Д. Б. Халяпин, В. И. Ярочкин. – М. : ИПКИР, 1994. – 128 с.

26. *Хорев, А. А.* Способы и средства защиты информации / А. А. Хорев. – М. : МО РФ, 1998. – 316 с.

27. *Ярочкин, В. И.* Технические каналы утечки информации / В. И. Ярочкин. – М. : ИПКИР, 1994. – 106 с.

Учебное издание

Комплексная защита объектов информатизации. Книга 13

СОКОЛОВ Алексей Игоревич
МОНАХОВ Михаил Юрьевич

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ
Технические каналы утечки информации

Учебное пособие

Подписано в печать 23.03.07.
Формат 60x84/16. Усл. печ. л. 5,11. Тираж 100 экз.
Заказ
Издательство
Владимирского государственного университета
60000, Владимир, ул. Горького, 87.