ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Б1. Б.2. 06 Инженерно-техническая защита информации и технические средства на критически важных объектах

Специальность 10.05.03 Информационная безопасность автоматизированных систем
Специализация Информационная безопасность автоматизированных систем критически важных объектов
Форма обучения очная

СОДЕРЖАНИЕ

1. КОНСПЕКТ ЛЕКЦИЙ

1. 1 Лекция № 1 (2 часа).

Тема: «Сущность и задачи инженерно-технической защиты информации. Классификация, структура и характеристики технических каналов утечки информации»

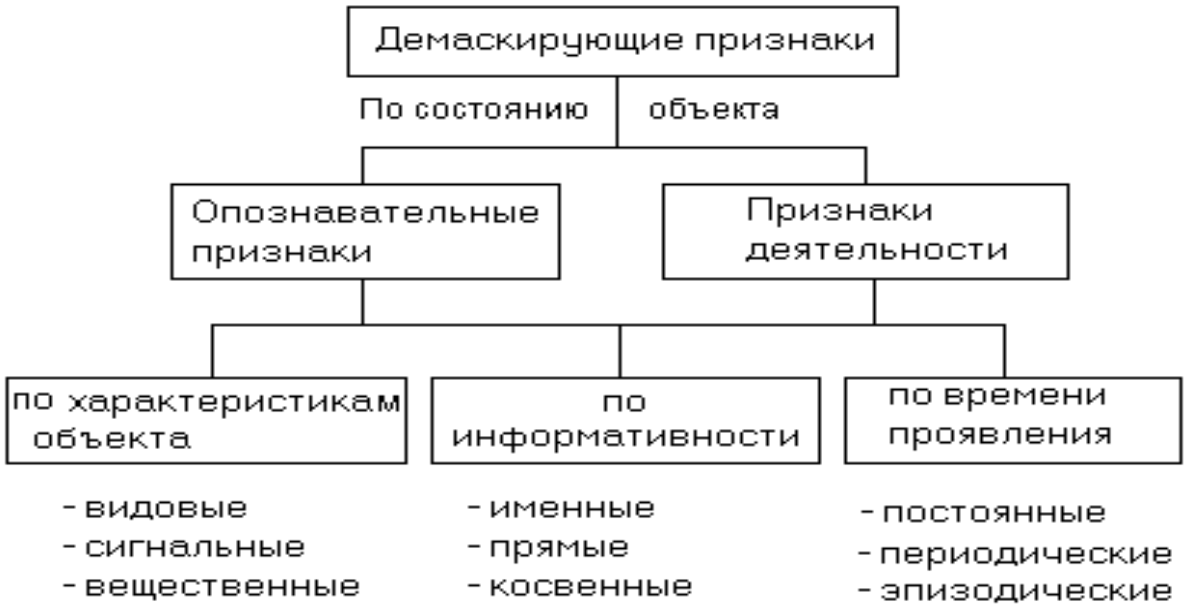
1.1.1 Вопросы лекции:

1. Демаскирующие признаки объектов.
2. Виды и структура технических каналов утечки информации
3. Характеристики каналов утечки информации

1.1.2 Краткое содержание вопросов:

1. Демаскирующие признаки объектов.

Признаки, позволяющие отличить один объект от другого, называются демаскирующими. Демаскирующие признаки объекта составляют часть его признаков, а значения их отличаются от значений соответствующих признаков других объектов.



К видовым признакам относятся форма объекта, его размеры, детали объекта, тон, цвет и структура его поверхности и др.

Признаки сигналов описывают параметры полей и электрических сигналов, генерируемых объектом: их мощность, частоту, вид (аналоговый, импульсный), ширину спектра и т. д.

Признаки веществ определяют физический и химический состав, структуру и свойства веществ материального объекта.

Важнейшим показателем признака является его **информативность.** Информативность признака оценивается мерой в интервале [0-1], характеризующей его индивидуальность.

Чем признак более индивидуален, т. е. принадлежит меньшему числу объектов, тем он более информативен.

Величину информативности можно определить как

$$I_k = (N - N_k) / N,$$

где N_k — количество объектов, содержащих признак **k**, из **N** рассматриваемых.

Опознавательные признаки описывают объекты в статическом состоянии: его назначение, принадлежность, параметры.

Признаки деятельности объектов характеризуют этапы и режимы

функционирования объектов, например, этап создания новой продукции: научные исследования, подготовка к производству, изготовление новой продукции, ее испытания и т. д.

Все признаки объекта по характеру проявления можно разделить на 3 группы:
- внешнего вида - видовые демаскирующие признаки;
- признаки излучений - сигнальные демаскирующие признаки;
- материально-вещественные признаки.

К видовым признакам относятся форма объекта, его размеры, детали объекта, тон, цвет и структура его поверхности и др.

Признаки излучений описывают параметры полей и электрических сигналов, генерируемых объектом: их мощность, частоту, вид (аналоговый, импульсный), ширину спектра и т. д.

Вещественные признаки определяют физический и химический состав, структуру и свойства веществ материального объекта.

Таким образом, совокупность демаскирующих признаков рассмотренных трех групп представляет модель объекта, описывающую его внешний вид, излучаемые им поля, внутреннюю структуру и химический состав содержащихся в нем веществ.

Под утечкой информации понимается несанкционированный процесс переноса информации от источника к злоумышленнику.

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 производится с помощью технических средств, то такой канал называется техническим каналом утечки.

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

Утечка информации по сравнению с утечкой (хищением) мате-риальных объектов имеет ряд особенностей, которые надо учиты-вать при организации защиты информации:

- при утечке информации не выполняются законы сохранения ма-терии, вследствие чего утечка не может быть обнаружена в ре-зультате уменьшения количества информации источника;
- утечка информации может происходить только при попадании ее к заинтересованному в ней несанкционированному получа-телю (злоумышленнику), в отличие, например, от утечки воды или газа;
- при утечке информации вследствие расширения круга ее потре-бителей цена информации уменьшается.

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

- при утечке информации не выполняются законы сохранения материи, вследствие чего утечка не может быть обнаружена в результате уменьшения количества информации источника;
- 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 вследствие расширения круга ее потребителей цена информации уменьшается.

2. Виды и структура технических каналов утечки информации

Обобщенная структура типового технического канала утечки

Для передачи информации носителями в виде полей и микрочастиц по любому техническому каналу (функциональному или каналу утечки) последний должен содержать 3 основные элемента: источник сигнала, среду распространения носителя и приемник.

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 волны, в том числе свет;
- объект наблюдения, излучающий собственные электромагнитные волны в оптическом и радиодиапазонах, вызванные тепловым движением электронов;
- движущиеся механизмы и машины, создающие акустические сигналы;
- передатчики функциональных каналов связи;
- ретрансляторы, например закладные устройства;
- источники побочных электромагнитных излучений и наводок (ПЭМИН);
- радиоактивные материалы.

Указанные на рисунке 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 производит преобразование этой формы 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, который переносят информацию;

– производит 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.

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

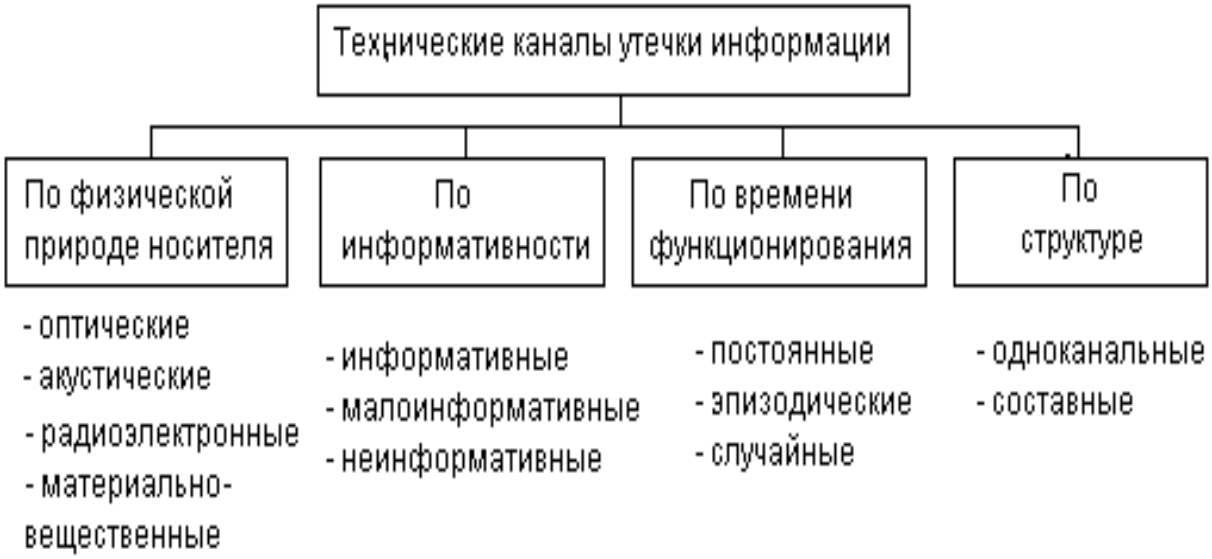
Среда распространения носителя - часть пространства, в которой перемещается носитель. Она характеризуется набором физических параметров, определяющих условия перемещения носителя с информацией. Среда распространения может быть в виде свободного пространства и направляющих линий. В качестве направляющих линий используются электрические провода различной конфигурации, волноводы, волоконно-оптические кабели, звукопроводы и другие конструкции.

Приемник выполняет функцию, обратные функции передатчика. Он производит:

- 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 усиление сигналов до значений, необходимых для безошибочного восприятия ими.

3. Характеристики каналов утечки информации

Классификация каналов утечки информации



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 каналу в единицу времени с определенным качеством. В теории связи пропускная способность канала в бодах (битах в секунду) определяется по формуле:

$$C=\Delta F \log_2 (1+P_c/P_п),$$

где ΔF-ширина полосы пропускания канала связи;

P_c 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.

1. 2 Лекция № 2 (2 часа).

Тема: «Оптические каналы утечки информации**»**

1.2.1 Вопросы лекции:

1. Структура оптического канала утечки информации
2. Характеристики среды распространения оптических лучей.
3. Основные показатели оптоэлектронных линий связи и способы снятия с них информации

1.2.2 Краткое содержание вопросов:

1. Структура оптического канала утечки информации

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, листы 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.

Мощность источника светового сигнала характеризуется величиной светового потока в **люменах (лм).**

Если объект наблюдается в отраженном свете, то создаваемый световой поток равен произведению освещенности объекта на площадь проекции объекта на плоскость, перпендикулярную направлению наблюдения. Освещенность измеряется в **люксах (лк)**

Источники оптических сигналов в видимом и ИК-диапазонах оптических каналов утечки информации характеризуются следующими показателями:

– диапазоном длин волн — 0,4-0,76 мкм в видимом диапазоне, 0,76-3 мкм — в ближнем, 3-6 мкм — в среднем, 8-14 мкм — в дальнем ИК-диапазонах;

– освещенностью объектов наблюдения внешним (солнечным) светом — 10^1-10^5 люкс (лк).

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).

При прохождении через атмосферу солнечные лучи взаимодействуют с содержащимися в ней молекулами газов, частицами пыли, дыма, кристалликами льда, каплями воды. В результате такого взаимодействия часть солнечной энергии поглощается, другая — рассеивается.

Процессы рассеяния и поглощения солнечной энергии уменьшают интенсивность солнечной радиации на поверхности Земли и меняют спектр солнечного света, освещающего наземные объекты.

Рассеяние в коротковолновой части спектра сильнее, чем в длинноволновой. Особенно заметно оно в голубой и ультрафиолетовой областях, поэтому небо имеет голубой цвет. Интенсивность рассеяния солнечного света в ближнем инфракрасном диапазоне незначительная.

Облачность существенно влияет на суммарную освещенность. Наличие облачности высоких ярусов, не закрывающих солнечный диск, повышает рассеянное излучение и при сохранении значения прямой освещенности увеличивает ее суммарную величину на 20-30% по сравнению с освещенностью при безоблачном небе. Низкая облачность так же, как и тени облаков, снижает в зависимости от высоты Солнца суммарную освещенность в 2-5 раз. При снежном покрове и облачности многократное отражение ими излучения повышает суммарную освещенность, особенно в теневых участках.

Освещенность в дневное время земной поверхности Солнцем зависит от его высоты и облачности атмосферы. 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.

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 не постоянен 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.

Средняя температура поверхности Земли близка к 17 ° по Цельсию. Максимум ее

теплового излучения приходится на длину волны, равную приблизительно 9,7 мкм. Объекты под действием солнечной радиации в течение дня по-разному отдают накопленное тепло в окружающее пространство. Различия в температуре излучения могут рассматриваться как демаскирующие признаки объекта.

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

Объект наблюдения в оптическом канале утечки информации может рассматриваться одновременно как источник информации и источник сигнала, так как световые лучи, несущие информацию о видовых признаках объекта, представляют собой отраженные объектом лучи внешнего источника или его собственные излучения.

Отраженный от объекта свет содержит информацию о внешнем виде (видовых признаках) объекта, а излучаемый объектом свет — о параметрах излучений (признаках сигналов). Запись информации производится в момент отражения падающего света путем изменения его яркости и спектрального состава. Излучаемый свет содержит информацию об уровне и спектральном составе источников видимого света, а в инфракрасном диапазоне по характеристикам излучений можно также судить о температуре элементов излучения

В видимом диапазоне мощность излучения определяется в подавляющем большинстве случаев мощностью отраженного света и содержащихся в объекте искусственных источников света.

2. Характеристики среды распространения оптических лучей.

Среду распространения в оптическом канале утечки информации образует:

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

Оптический канал утечки информации, среда распространения которого содержит участки безвоздушного пространства, возникает при наблюдении за наземными объектами с космических аппаратов.

Сложный состав атмосферы вызывает неравномерность (изрезанность) ее амплитудно-частотной характеристики как среды распространения. Участки в ней с малым затуханием называются окнами прозрачности.

В общем случае прозрачность атмосферы зависит от соотношения длины проходящего сквозь нее света и размеров взвешенных в атмосфере частиц. Если размеры частиц соизмеримы с длиной волны света (больше половины длины волны) или больше, то пропускание значительно ухудшается. Поэтому уровень пропускания меняется в зависимости от длины световой волны.

Прозрачность атмосферы среды распространения света оценивается метеорологической дальностью видимости. Метеорологическая видимость даже в окнах прозрачности зависит от наличия в атмосфере взвешенных частиц пыли и влаги, образующих мглу и туман, капелек и кристаллов воды в виде дождя и снега, а также аэрозолей и дымов, содержащих твердые частицы. Все это вызывает замутнение атмосферы и ухудшает видимость. Под метеорологической дальностью видимости понимается предельно большое расстояние, начиная с которого при данной прозрачности атмосферы в светлое время суток абсолютно черный предмет с угловыми размерами 20' х 20‘(угловых минут) сливается с фоном у горизонта и становится невидимым.

Если объект наблюдения и наблюдатель находятся на Земле, то протяженность

канала утечки зависит не только от состояния атмосферы, но и ограничивается влиянием кривизны Земли. Дальность прямой видимости $D_{пВ}$ в км с учетом кривизны Земли можно рассчитать по формуле:

$$D_{пв} = 3{,}57(\sqrt{h_o} + \sqrt{h_н}),$$

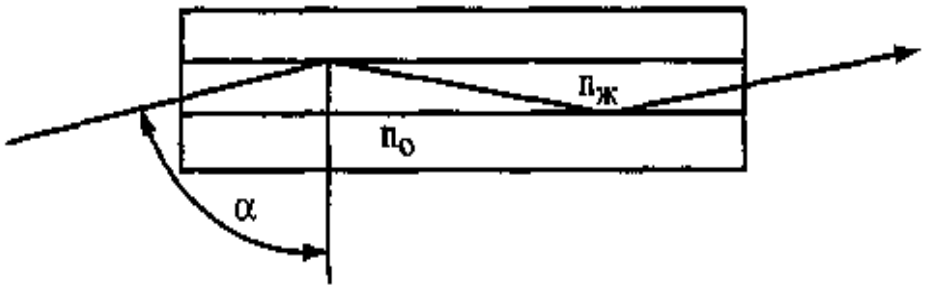
– где h_o— высота размещения объекта над поверхностью Земли в м; $h_н$— высота расположения наблюдателя над поверхностью Земли в м.

– Например, для h_o = 3 м и $h_н$ =5м $D_{пВ}$ = 14 км, что меньше метеорологической дальности при хорошей видимости. Эта формула не учитывает неровности поверхности Земли, растительность и различные инженерные сооружения (деревья, башни, высотные здания и т. д.), создающие препятствия для света.

В общем случае потенциальные оптические каналы утечки информации имеют достаточно устойчивые признаки.

До недавнего времени атмосфера и безвоздушное пространство были единственной средой распространения световых волн. С разработкой волоконно-оптической технологии появились направляющие линии связи в оптическом диапазоне, которые в силу больших их преимуществ по сравнению с традиционными электрическими проводниками рассматриваются как более совершенная физическая среда для передачи больших объемов информации. Линии связи, использующие оптическое волокно — волоконно-оптические линии связи (ВОЛС), устойчивы к внешним помехам, имеют малое затухание, долговечны, обеспечивают значительно большую безопасность передаваемой по волокну информации.

Волокно представляет собой нить диаметром около 100 мкм, изготовленную из кварца на основе двуокиси кремния. Волокно состоит из сердцевины (световодной жилы) и оболочки из оптически менее плотного кварца. Значения показателей преломления (отношений скорости света в вакууме к скорости распространения света в среде) жилы и оболочки выбираются такими, чтобы обеспечить полное отражение света, распространяющегося по световодной жиле, от границы между жилой и оболочкой.

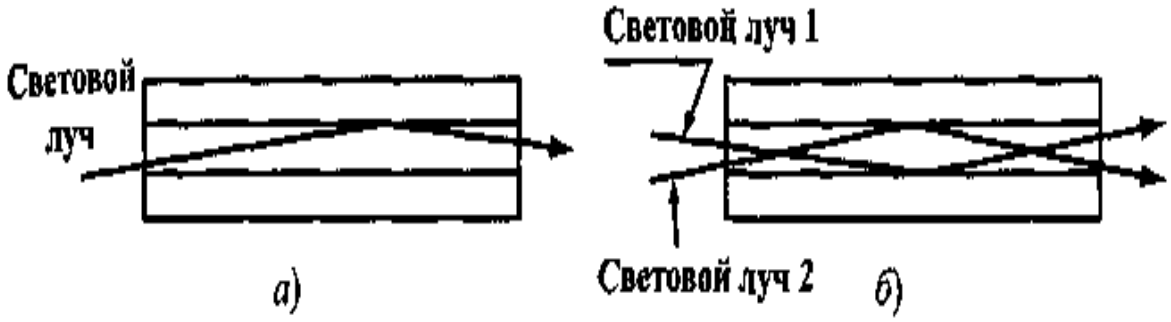


Предельный угол полного отражения света (угол падения света на границу раздела среды, при равенстве и превышении которого наблюдается полное отражение от него) определяется из соотношения $a = \arcsin(n_ж/n_o)$,

где $n_ж$; n_o — показатели преломления жилы и оболочки.

Волокно, у которого сердцевина имеет постоянный показатель преломления света, называется ступенчатым. Если показатель преломления жилы меняется, то волокно называется градиентным.

Для передачи оптических сигналов применяются два вида волокна: одномодовое и многомодовое. В одномодовом волокне световодная жила имеет диаметр порядка 8-10 мкм, по которой может распространяться один луч (одна мода) (рис. а)). В многомодовом волокне диаметр световодной жилы составляет 50-60 мкм, что делает возможным распространение в нем большого числа лучей (рис. б)).



Оптическое волокно как среда распространения оптического канала утечки информации характеризуется двумя основными параметрами: затуханием и дисперсией.

Затухание определяет потери света в результате его поглощения и рассеяния и измеряется в децибелах на километр (дБ/км).

Потери на поглощение зависят от чистоты материала и длины волны света, а потери на рассеяние — от неоднородности показателя преломления.

Кварц, так же как и воздух, имеет неравномерную амплитудно-частотную характеристику, с окнами прозрачности. Повышенная прозрачность кварца наблюдается в диапазонах 0,85 мкм, 1,3 мкм, 1,55 мкм и др.

Поэтому в качестве носителя информации применяется свет в этих диапазонах. Лучшие образцы волокна имеют затухание порядка 0,15-0,2 дБ/км, разрабатываются еще более «прозрачные» волокна с теоретическими значениями затухания порядка 0,02 дБ/км для волны длиной 2,5 мкм.

При таком затухании сигнала могут передаваться на расстояние в сотни км без ретрансляции (регенерации), что существенно превышает длину аналогичных линий связи на электрических проводах.

Волокна объединяют в волоконно-оптические кабели, покрытые защитной оболочкой. По условиям эксплуатации кабели подразделяются на монтажные, станционные, зоновые и магистральные. Кабели первых двух типов используются внутри зданий и сооружений. Зоновые и магистральные кабели прокладываются в колодцах кабельных коммуникаций, в грунтах, на опорах, под водой.

Малые размеры жилы световолокна и необходимость обеспечения центрирования жил и параллельности поверхностей торцов волокон при их соединении создают определенные трудности при коммутации и ремонте ВОЛС по сравнению с электрическими проводами. Для соединения волокон с приемно-передающей аппаратурой используются коннекторы (соединители) различных типов с накидной гайкой и защелками-фиксаторами. Затухание оптического сигнала в коннекторах составляет) доли дБ. Волокна сращиваются путем сварки, механического соединения с помощью специальных пластиковых устройств, представляющих соединения в прецизионной втулке с гелем, оптические свойства которого совпадают с оптическими свойствами волокна.

Хотя возможность утечки информации из волоконно-оптического кабеля существенно ниже, чем из электрического, но при определенных условиях такая утечка возможна. 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.

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.

3. Основные показатели оптоэлектронных линий связи и способы снятия с них информации

Показатели оптического приемника существенно влияют на характеристики оптических каналов утечки информации. Наиболее существенные для добывания информации из них следующие:

- диапазон длин волн, воспринимаемых оптическим приемником;
- чувствительность, определяемая минимальным уровнем светового потока на входе оптического приемника, при котором на его выходе формируется изображение объекта с приемлемым для злоумышленников качеством;
- разрешающая способность, характеризующая минимальные размеры точки (пикселя) изображения;
- угол (поле) зрения, определяющий наблюдаемую часть пространства;
- величина геометрических и цветовых искажений изображения объекта наблюдения.

От этих показателей зависит возможность добывания видовых демаскирующих признаков объекта наблюдения в различных участках оптического диапазона длин волн, дальность наблюдения объекта, точность измерения демаскирующих признаков, количество объектов на изображении.

1. 3 Лекция № 3 (2 часа).

Тема: «Акустические каналы утечки информации»

1.3.1 Вопросы лекции:

1. Классификация акустических каналов утечки информации.
2. Заходовые методы снятия информации.
3. Беззаходовые методы снятия информации

1.3.2 Краткое содержание вопросов:

1. Классификация акустических каналов утечки информации.

Целью данного занятия является рассмотрение способов добывания КИ путем подслушивания.

Актуальность использования таких каналов для съема информации широко представлена во многих художественных фильмах

Вспомнить классификацию, отметить место акустического КУИ среди остальных.

Звуком *называются механические колебание частиц упругой среды (воздуха, воды, металла и т.д.), субъективно воспринимаемые органом слуха. Звуковые ощущения вызываются колебаниями среды, происходящими в диапазоне частот от 16 до 20000 Гц.*

Звуковое давление *— это переменное давление в среде, обусловленное распространением в ней звуковых волн. Величина звукового давления Р оценивается силой действия звуковой волны на единицу площади и выражается в ньютонах на квадратный метр .*

Уровень звукового давления отношение величины звукового давления Р к нулевому уровню, за который принято звуковое давление $P= 2 \cdot 10^{-5}$ Н/м2

$N = 20 \lg P/P_0$

Сила (интенсивность) звука *— количество звуковой энергии, проходящей за единицу времени через единицу площади; измеряется в ваттах на квадратный метр (Вт/м2). Следует отметить, что звуковое давление и сила звука связаны между собой квадратичной зависимостью, т.е. увеличение звукового давления в 2 раза приводит к увеличению силы звука в 4 раза.*

Уровень силы звука *— отношение силы данного звука I к нулевому (стандартному) уровню, за который принята сила звука $I_0= 10^{-12}$ Вт/м2, выраженное в децибелах (дБ)*

$N = 10 \lg I/ I_0$

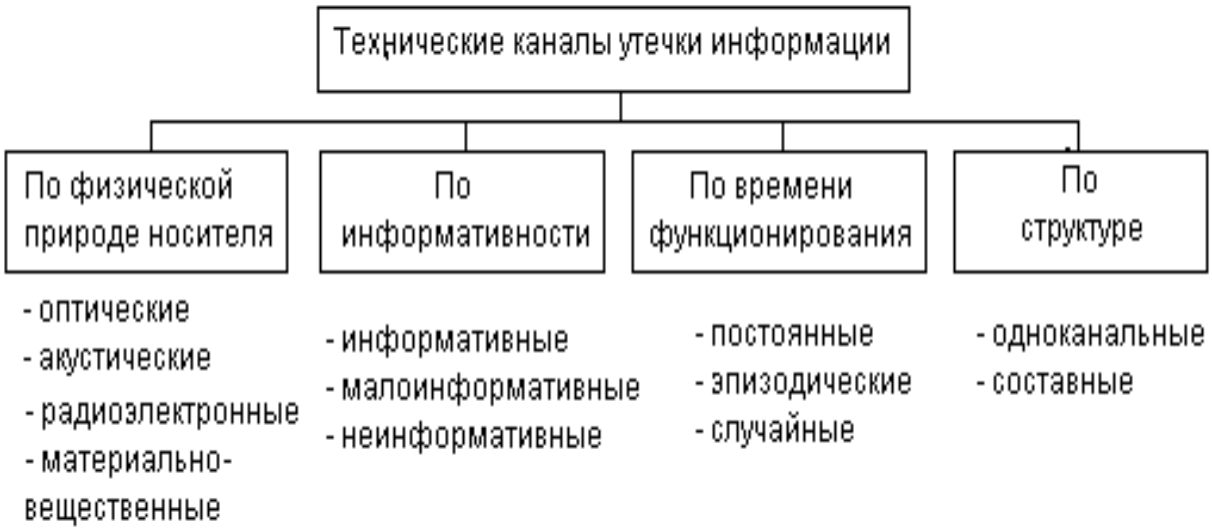
Уровни звукового давления и силы звука, выраженные в децибелах, совпадают по величине.

Порог слышимости *— наиболее тихий звук, который еще способен слышать человек на частоте 1000 Гц, что соответствует звуковому давлению $2 \cdot 10^{-5}$ Н/м2.*

Громкость звука *— интенсивность звукового ощущения, вызванная данным звуком у человека с нормальным слухом. Громкость зависит от силы звука и его частоты, измеряется пропорционально логарифму силы звука и выражается количеством децибел, на* которое данный звук превышает по интенсивности звук, принятый за порог слышимости. Единица измерения громкости — фон.

Динамический диапазон *— диапазон громкостей звука или разность уровней звукового давления самого громкого и самого тихого звуков, выраженная в децибелах.*

Диапазон основных звуковых частот речи лежит в пределах от 70 до 1500 Гц. Однако с учетом обертонов речевой диапазон звучания расширяется до 5000–8000 Гц (рис. 6.1). У русской речи максимум динамического диапазона находится в области частот 300–400 Гц



Источником образования акустического канала утечки информации являются вибрирующие, колеблющиеся тела и механизмы, такие как голосовые связки человека,

движущиеся элементы машин, телефонные аппараты, звукоусилительные системы и т.д.

Распространение звука в пространстве осуществляется звуковыми волнами. *Упругими, или механическими, волнами называются механические возмущения (деформации), распространяющиеся в упругой среде. Тела, которые, воздействуя на среду, вызывают эти возмущения, называются источниками волн. Распространение упругих волн в среде не связано с переносом вещества. В неограниченной среде оно состоит в вовлечении в вынужденные колебания все более и более удаленных от источника волн частей среды.*

Упругая волна является продольной и связана с объемной деформацией упругой среды, вследствие чего может распространяться в любой среде — твердой, жидкой и газообразной.

Когда в воздухе распространяется акустическая волна, его частицы образуют упругую волну и приобретают колебательное движение, распространяясь во все стороны, если на их пути нет препятствий. В условиях помещений или иных ограниченных пространств на пути звуковых волн возникает множество препятствий, на которые волны оказывают переменное давление (двери, окна, стены, потолки, полы и т.п.), приводя их в колебательный режим. Это воздействие звуковых волн и является причиной образования акустического канала утечки информации.

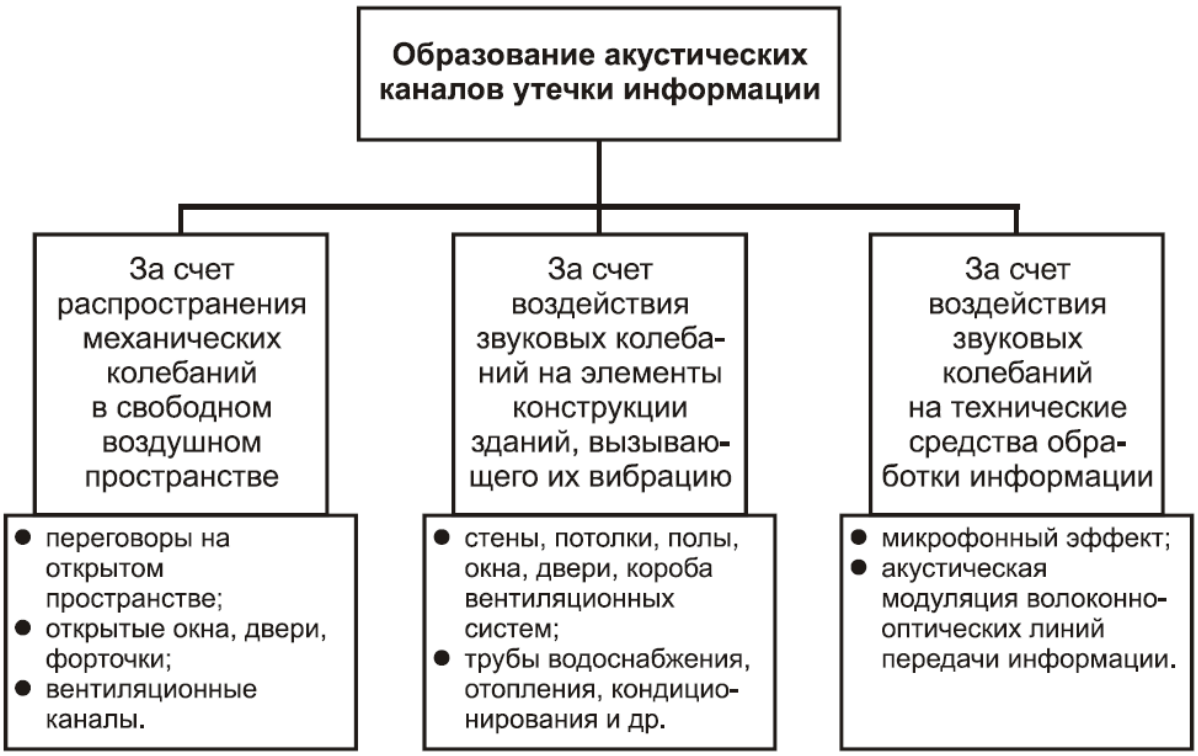
Акустические каналы утечки информации образуются за счет:

- распространение акустических колебаний в свободном воздушном пространстве;
- воздействия звуковых колебаний на элементы и конструкции зданий;
- воздействия звуковых колебаний на технические средства обработки информации.

Механические колебания стен, перекрытий, трубопроводов, возникающие в одном месте от воздействия на них источников звука, передаются по строительным конструкциям на значительные расстояния, почти не затухая, не ослабляясь, и излучаются в воздух как слышимый звук. Опасность такого акустического канала утечки информации по элементам здания состоит в большой и неконтролируемой дальности распространения звуковых волн, преобразованных в упругие продольные волны в стенах и перекрытиях, что позволяет прослушивать разговоры на значительных расстояниях.

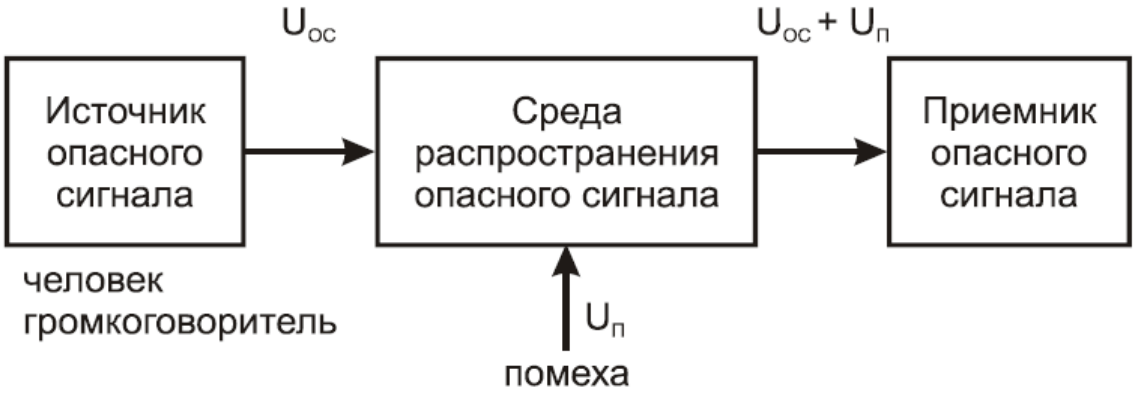
Еще один канал утечки акустической информации образуют системы воздушной

вентиляции помещений, различные вытяжные системы и системы подачи чистого воздуха. Возможности образования таких каналов определяются конструктивными особенностями воздуховодов и акустическими характеристиками их элементов: задвижек, переходов, распределителей и др.



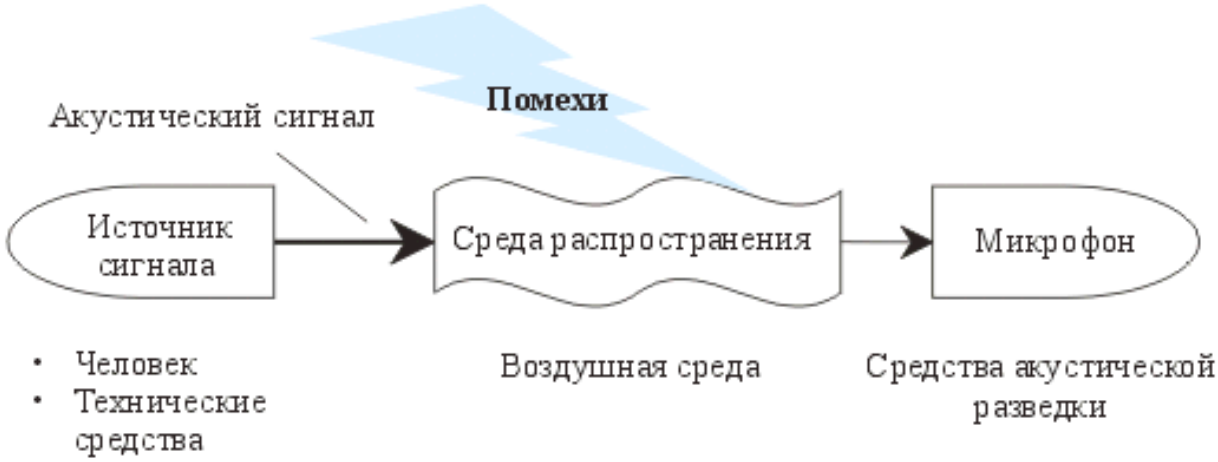
Среды распространения речевой информации по способу переноса звуковых волн делятся на:

- среды с воздушным переносом;
- среды с материальным переносом (монолит);
- среды с мембранным переносом (колебания стекол).



В зависимости от физической природы возникновения информационных сигналов, среды распространения акустических колебаний и способов их перехвата, акустические каналы утечки информации также можно разделить на воздушные, вибрационные, электроакустические, оптико-электронные и параметрические.

В воздушных технических каналах утечки информации средой распространения акустических сигналов является воздух, а для их перехвата исполь-зуются миниатюрные высокочувствительные микрофоны и специальные направлен-ные микрофоны.



Микрофоны объединяются или соединяются с портативными звукозаписывающими устройствами (диктофонами) или специальными миниатюрными передатчиками

В вибрационных (структурных) каналах утечки информации средой распространения акустических сигналов являются конструкции зданий, сооружений (стены, потолки, полы), трубы водоснабжения, отопления, канализации и другие твёрдые тела. Для перехвата акустических колебаний в этом случае исполь-зуются контактные микрофоны (стетоскопы).

Электроакустические технические каналы утечки информации возникают за счет электроакустических преобразований акустических сигналов в электрические. Перехват акустических колебаний осуществляется через ВТСС, обладающие “микрофонным эффектом”, а также путем “высокочастотного навязывания”.

Оптико-электронный (лазерный) канал утечки инфор-мации образуется при облучении лазерным лучом вибрирующих в акустическом по-ле тонких отражающих поверхностей (стекол, окон, картин, зеркал и т.д.).

Отраженное лазерное излучение (диффузное или зеркальное) модулируется по амплитуде и фазе (по закону вибрации поверхности) и принимается приемником оптического излучения, при демодуляции которого выделяется речевая информация.

В результате воздействия акустического поля меняется давление на все элементы высокочастотных генераторов ТСПИ и ВТСС. При этом изменяется (незначительно) взаимное расположение элементов схем, проводов в катушках индуктивности, дросселей и т.п., что может привести к изменениям параметров высокочастотного сигнала, например, к модуляции его информационным сигналом. Поэтому этот канал утечки информации называется параметрическим.

Это обусловлено тем, что незначительное изменение взаимного расположения проводов в катушках индуктивности (межвиткового расстояния) приводит к изменению их индуктивности, а, следовательно, к изменению частоты излучения генератора, т.е. к частотной модуляции сигнала. Точно так же воздействие акустического поля на конденсаторы приводит к изменению расстояния между пластинами и, следовательно, к изменению его емкости, что, в свою очередь, также приводит к частотной модуляции высокочастотного сигнала генерации.

2. Заходовые методы снятия информации.

Перехват акустической информации с помощью радиопередающих средств. К ним относится широкая номенклатура радиозакладок (радиомикрофонов, “жучков”), назначением которых является передача по радиоканалу акустической информации, получаемой на объекте.

Применение радиопередающих средств предполагает обязательное наличие приемника, с помощью которого осуществляется прием информации от радиозакладки.

Приемники используются разные — от бытовых (диапазон 88–108 МГц) до специальных. Иногда применяются так называемые автоматические станции. Они предназначены для автоматической записи информации в случае ее появления на объекте.

Передача информации может осуществляется по ИК каналу. Акустические закладки данного типа характеризуются крайней сложностью их обнаружения. Срок работы этих изделий — несколько суток, но следует иметь в виду, что прослушать их передачу можно лишь на спецприемнике и только в прямом визуальном контакте, т.е. непосредственно видя эту закладку. Поэтому размещаются они у окон, вентиляционных отверстий и т.п., что облегчает задачу их поиска. Основное достоинство этих закладок — скрытность их работы.

Сходство этих закладок в том, что они используют в своей работе принцип низкочастотного уплотнения канала передачи информации. Поскольку в “чистых” линиях (220 В) и телефонных линиях присутствуют только сигналы на частотах 50 Гц и 300–3500 Гц соответственно, то передатчики таких закладок, транслируя свою информацию на частотах 100–250 кГц, не мешают работе этих сетей. Подключив к этим линиям спецприемники, можно снимать передаваемую с закладки информацию на дальность до 500 м.

Диктофоны — устройства, записывающие голосовую информацию на магнитный носитель (ленту, проволоку, внутреннюю микросхему памяти). Время записи различных диктофонов колеблется в пределах от 15 мин до 8 ч.

Современные цифровые диктофоны записывают информации во внутреннюю память, позволяющую производить запись разговора длительностью до нескольких часов. Эти диктофоны практически бесшумны (т.к. нет ни кассеты, ни механического лентопротяжного механизма, производящих основной шум), имеют возможность сброса записанной информации в память компьютера для ее дальнейшей обработки (повышения разборчивости речи, выделения полезных фоновых сигналов и т.д.).

Проводные микрофоны устанавливаются в интересующем помещении и соединяются проводной линией с приемным устройством. Микрофоны устанавливаются либо скрытно (немаскированые), либо маскируются под предметы обихода, офисной техники и т.д. Такие системы обеспечивают передачу аудиосигнала на дальность до 20 м. При использовании активных микрофонов — до 150 м. Несколько микрофонов могут заводиться на общее коммутирующее устройство, позволяющее одновременно контролировать несколько и осуществляющее запись перехваченных разговоров на диктофон.

Данное устройство обычно скрытно монтируется либо в телефоне, либо в телефонной розетке. Работает оно следующим образом. Человек, который хочет воспользоваться данным устройством (оператор), производит телефонный звонок по номеру, на котором оно “висит”. “Телефонное ухо” (“ТУ”) “проглатывает” первые два звонка, т.е. в контролируемом помещении телефонные звонки не раздаются. Оператор кладет трубку и опять набирает этот номер. В трубке будет звучать сигнал “занято”, оператор ждет 30-60 с (временной пароль) и после прекращения сигнала “занято” набирает бипером (генератором DTMF-посылок) заданную кодовую комбинацию (цифровой пароль). После этого включается микрофон “ТУ” и оператор слышит все, что происходит в контролируемом помещении практически из любой точки мира, где есть телефонный аппарат. Разрыв связи произойдет, если оператор положит трубку или если кто-то поднимет телефонную трубку в контролируемом помещении. Для всех остальных абонентов, желающих дозвониться по этому номеру, будет слышен сигнал “занято”. Данный алгоритм работы является типовым, но может отличаться в деталях реализации, в зависимости от требований.

3. Беззаходовые методы снятия информации

Прослушивание помещений через телефон осуществляется за счет использования “микрофонного эффекта”.

ВЧ колебания проходят через микрофон или детали телефона, обладающие “микрофонным эффектом” и модулируются в акустический сигнал из помещения, где установлен телефонный аппарат. Промодулированый сигнал демодулируется амплитудным детектором и после усиления подается на регистрирующее устройство.

Этот канал утечки речевой информации представляет опасность еще и с точки зрения сложности его обнаружения службой безопасности объекта. Поскольку уровни излучений очень малы, зафиксировать их без составления радиокарты практически нереально.

Стетоскопы — это устройства, преобразующие упругие механические колебания твердых физических сред в акустический сигнал. В современных стетоскопах в качестве такого преобразователя служит пьезодатчик. Данная аппаратура в основном применяется для прослушивания соседних помещений через стены, потолки, пол или через трубы центрального отопления. Профессиональная аппаратура этого класса компактна (помещается в кейсе средних размеров), автономна, имеет возможность подстройки параметров под конкретную рабочую обстановку, осуществляет запись полученной информации на диктофон.

Стетоскопические датчики часто дооборудуются радиопередатчиком, что позволяет прослушивать перехваченную информацию на сканирующий приемник, как от обычной радиозакладки.

Лазерные стетоскопы — это устройства, позволяющие считывать лазерным лучом вибрацию с предметов, промодулированых акустическим сигналом. Обычно акустическая информация снимается с оконных стекол. Современные лазерные стетоскопы хорошо работают на дальности до 300 м. Недостатками этой аппаратуры являются высокая стоимость (до 30 тыс. долларов), необходимость пространственного разноса источника и приемника лазерного излучения, сильная зависимость качества работы от внешних условий (метеоусловия, солнечные блики и т.д.).

Данная техника предназначена для прослушивания акустической информации с определенного направления и с больших расстояний. В зависимости от конструкции НАМ, ширина главного луча диаграммы направленности находится в пределах 5–30°, величина коэффициента усиления 5–20. По типу используемых антенных систем НАМ бывают.

Зеркальные (микрофон НАМ находится в фокусе параболической антенны). Расстояние 500 м и более, диаметр зеркала составляет до 1 м, диаграмма направленности — до 8°.

Микрофон-трубка (обычно маскируется под трость или зонт), при этом дальность действия до 300 м, а диаграмма направленности — до 18°. При повышении уровня шумов до 60 дБ дальность снижается до 100 м.

Плоский микрофон представляет собой фазированную акустическую решетку, в узлах которой размещаются микрофоны, сигналы которых суммируются на входе усилителя. Число приемных точек в таких решетках составляет несколько десятков. Конструктивно плоские фазированные решетки встраиваются либо в переднюю стенку атташе-кейса, либо в майку-жилет, которая надевается под рубашку и т.п. Необходимые электронные блоки могут располагаться также в кейсе, либо под одеждой. Таким образом, плоские фазированные решетки с камуфляжем визуально более незаметны по сравнению с параболическим микрофоном.

Способы реализации рассмотренных методов могут использоваться в различных случаях.

1. 4 Лекция № 4 (2 часа).

Тема: «Радиоэлектронные каналы утечки информации. Каналы утечки информации, обрабатываемой средствами вычислительной техники**»**

1.4.1 Вопросы лекции:

1. Особенности радиоэлектронных каналов утечки информации.
2. Виды и структура радиоэлектронных каналов утечки информации.
3. Направляющие линии связи, их характеристики.

1.4.2 Краткое содержание вопросов:

1. Особенности радиоэлектронных каналов утечки информации.

В радиоэлектронном канале передачи носителем информации является электрический ток и электромагнитное поле с частотами колебаний от звукового диапазона до десятков ГГц.

Радиоэлектронный канал относится к наиболее информативным каналам утечки в силу следующих его особенностей:

- независимости функционирования канала от времени суток и года, существенно меньшая зависимость его параметров по сравнению с другими каналами от метеоусловий;
- высокой достоверности добываемой информации, особенно при перехвате ее в функциональных каналах связи (за исключением случаев дезинформации);
- большого объема добываемой информации;
- оперативности получения информации вплоть до реального масштаба времени;
- скрытности перехвата сигналов и радиотеплового наблюдения.

В радиоэлектронном канале производится перехват радио- и электрических сигналов, а также радиолокационное и радиотеплолокационное наблюдение.

Следовательно, в рамках этого кана-ла утечки добывается семантическая информация, видовые и сиг-нальные демаскирующие признаки.

Радиоэлектронные каналы утечки информации используют радио-, радиотехническая, радио-локационная и радиотепловая разведка.

2. Виды и структура радиоэлектронных каналов утечки информации.

Структура радиоэлектронного канала утечки информации в общем случае включает источник сигнала или передатчик, среду распространения электрического тока или электромагнитной волны и приемник сигнала.

Радиоэлектронные каналы в зависимости от вида источников сигналов можно разделить на каналы 1 и 2-го вида. В каналах утечки первого вида производится перехват информации, передаваемой по функциональному каналу связи.

С этой целью приемник сигнала канала утечки информации настраивается на параметры сигнала или подключается (контактно или дистанционно) к проводам соответствующего канала связи. Такой канал Утечки имеет общий с функциональным каналом связи источник сигналов — передатчик и часть среды радиоканала или проводнофункционального канала до точки подключения средства съема.

Перехватываемые сигналы передающих устройств функциональных каналов связи имеют мощность от долей Вт до миллиона Вт (МВт). Но так как места расположения приемников функционального канала и канала утечки информации в общем случае не совпадают, то перехватываемый сигнал имеет меньшую мощность, чем сигнал на входе приемника функционального канала связи.

Радиоэлектронный канал утечки 2-го вида имеет собственный набор элементов: передатчик сигналов, среду распространения и приемник сигналов.

Передатчик сигналов этого канала утечки информации образуется случайно (без участия источника или получателя информации) или специально устанавливается в помещении злоумышленником. Такими передатчиками могут быть случайные источники опасных сигналов и закладные устройства. Опасные сигналы, как отмечалось ранее, возникают в результате акустоэлектрических преобразований, побочных низкочастотных и высокочастотных полей, паразитных связей и наводок в проводах и элементах радиосредств. Предпосылки для них создаются в результате конструктивных недоработок

при разработке радиоэлектронного средства, объективных физических процессов в их элементах, изменениях параметров в них из-за старения или нарушений правил эксплуатации, неучете полей вокруг средств или токонесущих проводов при их прокладке в здании и т. д.

Особенностями передатчиков канала 2-го вида являются малые уровни электрических сигналов — единицы и доли мВ и мощность радиосигналов, не превышающая десятки мВт (для радиозакладок). В результате этого протяженность таких каналов невелика и составляет десятки и сотни метров. Поэтому для добывания информации с использованием такого канала утечки приемник необходимо приблизить к источнику на величину длины канала утечки или установить ретранслятор.

Средой распространения сигналов радиоэлектронного канала утечки информации являются атмосфера, безвоздушное пространство (для канала 1-го вида) и направляющие — электрические провода различных типов и волноводы. Носитель в виде электрического тока распространяется по проводам, а электромагнитное поле — в атмосфере, в безвоздушном пространстве или по направляющим — волноводам. В приемнике производится выделение (селекция) носителя с интересующей получателя информацией по частоте, усиление выделенного слабого сигнала и съем с него информации — демодуляция.

Среда распространения радиоэлектронных каналов утечки существенно различается для электрических и радиосигналов. Электрические сигналы как носители информации могут быть аналоговыми или дискретными, их спектр может содержать частоты от десятков Гц до десятков ГГц. Электрические сигналы распространяются по направляющим линиям связи, связывающим источники и приемники сигналов как внутри организации, так внутри населенного пункта, города, страны, земного шара в целом. Способы и средства передачи электрических сигналов по проводам рассматриваются теорией и техникой проводной связи.

3. Направляющие линии связи, их характеристики.

Основными параметрами проводных линий связи являются ширина пропускаемого ими спектра частот и собственное зату-хание.

Если сопротивление проводни-ков на низких частотах (в звуковом диапазоне) определяется удель-ным сопротивлением материала и площадью поперечного сечения проводника, то на более высоких частотах начинается сказывать-ся влияние поверхностного эффекта. Сущность его заключает-ся в том, что переменное магнитное поле, возникающее при про-текании по проводнику тока, создает внутри проводника вихре-вые токи. В результате этого плотность основного тока перерас-пределяется по сечению проводника (жилы): уменьшается в цент-ре и возрастает на периферии.

На величину затухания линии влияют также электрические характеристики диэлектрика, наносимого на металлические провода. За счет их удается расширить полосу пропускания линии. При передаче по воздушным линиям со стальными проводами шири-на пропускания составляет около 25 кГц, с медными проводами — до 150 кГц, по симметричным кабелям — до 600 кГц. Расширению спектра частот, передаваемых по симметричным цепям, препятс-твуют возрастающие наводки. Например, удовлетворительным для телефонных линий считается значение переходного затухания порядка 60-70 дБ.

Металлические волноводы представляют собой трубы прямоугольного или круглого сечения, внутри которых может распространяться электромагнитное поле от излучателя, установленного в торце одной из сторон волновода. Волноводы применяются для передачи электромагнитного поля с длиной волны короче 10-15 см. Отражаясь от внутренней поверхности волновода, электромагнитное поле концентрируется в волноводе и при движении повторяет его изгибы. С целью уменьшения затухания электромагнитного

поля внутренние стенки волновода покрывают тонким слоем серебра. Кроме медных и алюминиевых находят применение волноводы из пластических масс с металлизированными изнутри стенками.

Другие типы направляющих линий представляют собой разновидности волноводных линий с иными физическими процессами. В металло-диэлектрических линиях связи электромагнитное поле распространяется в виде поверхностной волны вдоль металлической ленты или цилиндрического провода с ребристой поверхностью. Энергия электромагнитного поля концентрируется в пространстве, окружающем такой волновод, затухая по мере удаления от него. Недостатком такого волновода является паразитное излучение в эфир электромагнитного поля.

Для передачи сантиметровых и миллиметровых волн могут служить диэлектрические волноводы, в которых поверхностью раздела, направляющей волну, служит внутренняя поверхность диэлектрического стержня волновода. Диэлектрические волноводы чувствительны к внешним воздействиям и создают дополнительные потери, связанные с просачиванием энергии за пределы волновода, что затрудняет их практическое применение.

Основным носителем информации в радиоэлектронном канале является электромагнитное поле.

Электромагнитное поле представляет форму движения материи в виде взаимосвязанных колебаний электрического и магнитного полей. Электромагнитное поле возникает при протекании по проводам источника радиосигнала электрического тока переменной частоты и распространяется с конечной скоростью в окружающем пространстве. Векторы напряженности электрического и магнитного полей взаимно перпендикулярны и перпендикулярны направлению распространения электромагнитной волны. Электромагнитная волна характеризуется частотой колебания, мощностью и поляризацией. По частоте электромагнитные волны классифицируются в соответствии с Регламентом радиосвязи, утвержденным на Всемирной административной конференции в Женеве в 1979 г.

При распространении радиоволн в городе характер их распространения существенно искажается по сравнению с распространением на открытых пространствах за счет многочисленных переотражений от стен зданий и помещений и затухания в них. Эти обстоятельства необходимо учитывать при оценке пространственной ориентации и возможностей каналов утечки информации.

Многообразие природных и искусственных источников излучений в радиодиапазоне порождает проблему электромагнитной совместимости радиосигналов с определенной информацией с другими радиосигналами — помехами с совпадающими частотами

Естественные или природные помехи имеют земное и внеземное происхождение. Земные помехи вызываются физическими процессами в атмосфере, Земле и объектах на ее поверхности, основные из которых следующие:

- электрические грозовые разряды на частотах, как правило, ме
  нее 30 Мгц;
- разряды статического электричества в облаках и атмосферных
  осадках;
- резонансные электрические колебания между Землей и ионосферой;
- тепловое излучение Земли и зданий в диапазоне более 30-40 МГц;
- тепловые шумы в элементах и цепях радиоприемников.

Внеземные помехи на частотах выше 1 МГц обусловлены комбинированным излучением Галактики с дискретным и сплошным спектром. Солнце является мощным источником электромагнитных излучений, особенно в период его высокой активности, в основном на частотах выше 20 МГц. Луна, Юпитер и сверхновая звезда Кассиопея-А представляют собой дополнительные источники космических помех в УКВ-диапазонах.

Другие источники естественных помех включают тепловое галактическое излучение, излучение ионизированного и нейтрального водорода и др. Земли достигают также помехи низкой интенсивности, обусловленные вспышками звезд и излучениями радиогалактик.

Обратной стороной технического прогресса является рост уровня искусственных помех. Наиболее интенсивные радиоизлучения создаются передающими устройствами различных радио- и радиотехнических средств (станций радиовещания и телевидения, радиолокации, радионавигации, связи и др.). В целях обеспечения их электромагнитной совместимости частоты радиодиапазонов закреплены международными соглашениями и нормативными документами между различными видами деятельности и средств.

К источникам непреднамеренных помех, возникающих в результате побочных физических эффектов работы технических средств, относятся различные генераторы и преобразователи электроэнергии, линии электропередач, промышленное оборудование, транспорт на электрической тяге, системы зажигания двигателей внутреннего сгорания, медицинское оборудование, сварочные аппараты, осветительные газоразрядные лампы и др.

Преднамеренные помехи создаются специально для подавления систем управления и связи противника в военное время и защиты своей информации от перехвата содержащих се радиосигналов радиоэлектронными средствами добывания. Так как эффективность боевых действий в современных условиях зависит от надежности и достоверности связи в войсках и управления оружием, то подавление их мощными помехами не менее, а иногда и более результативно, чем применение оружия. Для ведения радиоэлектронной борьбы в вооруженных силах существует специальный род войск. Электромагнитное зашумление с целью защиты информации создается также генераторами помех, размещаемых в помещениях, в которых циркулирует защищаемая информация.

Маскирующие помехи создают помеховый фон, на котором затрудняется или исключается обнаружение и распознавание полезных сигналов. Имитирующие помехи по структуре близки к полезным сигналам и при приеме могут ввести в заблуждение получателя. С этой целью электромагнитные колебания помех модулируются по амплитуде и частоте (фазе), изменяются параметры импульсных помех, вызывающих срыв слежения в импульсных радиолокационных станциях управления оружием и определения координат целей.

По виду сигнала помехи делятся на флуктуационные, гармонические и импульсные. Флуктуационные помехи имеют распределенный по частоте спектр и создаются коронами высоковольтных линий электропередач, лампами дневного света, неоновой рекламой, электросваркой и другими электрическими разрядами. Спектр промышленных гармонических помех локализован на частотах излучений, возникающих при нелинейных преобразованиях в промышленных установках. Импульсные помехи, возникающие, прежде всего, при замыкании и размыкании электрических контактов выключателей, характеризуются сосредоточением энергии электромагнитных излучений в короткий промежуток времени.

Так как электромагнитные волны в радиодиапазоне являются основными носителями информации, то с целью нарушения управления и связи в ходе радиоэлектронной борьбы созданы разнообразные средства генерирования помех.

По соотношению спектра помех и полезных сигналов помехи подразделяются назаградительные и прицельные. Заградительные помехи имеют ширину спектра частот, значительно превышающую ширину спектра полезного сигнала, что позволяет подавлять сигнал без точной настройки генератора помех на его частоту.

Прицельная помеха имеет ширину спектра, соизмеримую (равную или превышающую в 1,5-2 раза) с шириной спектра сигнала, и создает высокий уровень спектральной плотности мощности в полосе частот сигнала при небольшой (относительно

мощности заградительной помехи) мощности передатчика помех.

Помеха изменяет демаскирующие признаки сигнала случайным образом (маскирующая помеха) или формирует демаскирующие признаки другого объекта сигнала (имитирующая помеха).

Помеха, которая зашумляет пространство, называется пространственной, а помеха, распространяющаяся по направляющим линиям, — линейной.

1. 5 Лекция № 5 (2 часа).

Тема: «Материально-вещественные каналы утечки информации»

1.5.1 Вопросы лекции:

1. Структура материально-вещественного канала утечки информации и характеристики ее элементов.
2. Способы утечки демаскирующих веществ в твердом, жидком и газообразном виде.
3. Особенности утечки информации о радиоактивных веществах.

1.5.2 Краткое содержание вопросов:

1. Структура материально-вещественного канала утечки информации и характеристики ее элементов.

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 (макротела и микрочастицы). 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.

Основными источниками информации вещественного канала утечки информации являются следующие:

- черновики различных документов и макеты материалов, узлов, блоков, устройств, разрабатываемых в ходе научно-исследовательских и опытно-конструкторских работ, ведущихся в организации;
- отходы делопроизводства и издательской деятельности в организации, в том числе использованная копировальная бумага, забракованные листы при оформлении документов и их размножении;
- отходы промышленного производства опытного и серийного выпуска продукции, содержащей защищаемую информацию в газообразном, жидком и твердом виде;
- содержащие защищаемую информацию дискеты и жесткие диски ПЭВМ, нечитаемые из-за их физических дефектов и искажений загрузочных или других секторов;
- бракованная продукция и ее элементы;
- радиоактивные материалы.

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

- людьми (сотрудниками организации, посетителями, представителями вторсырья и др.) и управляемыми ими техническими средствами;
- 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.

2. Способы утечки демаскирующих веществ в твердом, жидком и газообразном виде.

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

В рамках вещественного канала ведется химическая и радиационная разведка. Демаскирующие вещества добываются в основном путем взятия проб веществ в твердой, жидкой и воздушной средах. Развиваются активные и пассивные методы и средства анализа веществ, в основном в воздушных средах. В активных методах предусматривается посылка лазерного луча к исследуемой воздушной смеси и анализ излучений результатов взаимодействия. В пассивных методах производится анализ спектра собственных излучений веществ.

Потери носителей с ценной информацией возможны при отсутствии в организации четкой системы учета ее носителей. 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 организации, а далее при перегрузке бака или транспортировке 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, технологические процессы которых сопровождаются использованием или получением различных газообразных или жидких веществ, 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, на траве и цветах в окрестностях 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 концентрация может превышать допустимые значения за счет накопления демаскирующих веществ в земле, растительности, 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.

3. Особенности утечки информации о радиоактивных веществах.

Утечка информации о радиоактивных веществах возможна в результате выноса

радиоактивных веществ сотрудниками органи-зации или регистрации злоумышленником их излучений с помо-щью соответствующих приборов.

Утечка информации о радиоактивных веществах возможна по двум каналам: оптическому, носителями информации в котором являют-ся электромагнитные поля в виде у-излучений, и вещественному, носителями информации в котором являются элементарные a- и b-частицы.

Дальность канала утечки информации о радиоактивных вещес-твах через их излучения невелика: для a-излучений она составля-ет в воздухе единицы мм, b-излучений — см, только у-излучения можно регистрировать на удалении в сотни и более метров от ис-точника излучения.

Вещественные признаки продукции, содержащие защищаемую информацию, определяются в результате химического, физико-химического и физического анализа. Основу химического анализа составляют химические реакции изучаемого вещества в растворе. Физико-химический анализ предусматривает измерение физических величин, изменение которых обусловлено химическими реакциями. Физический анализ учитывает изменение физических характеристик добытой пробы, вызванных исследуемым веществом.

Принципы и методы определения химического состава вещества рассматривает аналитическая химия, которая включает качественные и количественные методы анализа. Для аналитической химии характерно применение не только традиционных химических методов, но и физико-химических и физических методов, а также биологических методов.

Качественный анализ представляет собой совокупность методов установления химического состава путем идентификации атомов, ионов, молекул, входящих в анализируемое вещество. Основными показателями качественного анализа являются специфичность и чувствительность. Специфичность характеризует возможность метода обнаруживать искомое вещество в присутствии других элементов. Чувствительность определяется наименьшим количеством вещества, которое может быть обнаружено рассматриваемым методом. Чувствительность современных методов качественного анализа составляет порядка 1 мкг.

Количественный анализ использует совокупность методов определения количественных соотношений, в которых находятся элементы или отдельные соединения в анализируемом веществе. Показатели количественного анализа — специфичность, чувствительность и точность. Чувствительность и точность измеряются в процентах содержания исследуемого вещества в пробе.

Основными методами аналитической химии являются:

- методы разделения веществ;
- термические методы;
- химические методы;
- электрохимические методы;
- хроматографические методы;
- спектральный анализ;
- масс-спектрографические методы;
- радиоактивные методы;
- биологические методы.

Разделение— операция, в результате которой отделяются один от другого компоненты, составляющие исходную смесь. Для разделения применяются такие процессы как:

- осаждение, основанное на различной растворимости соединений в водных растворах;
- экстракция — процесс распределения вещества между двумя фазами;
- сорбция — поглощение газов, паров или растворенных веществ твердыми или жидкими поглотителями — сорбентами;

- электровыделение (электролиз), при котором отделяемое вещество выделяют на твердых электродах;
- электрофорез, основанный на различиях в скоростях движения частиц разного заряда, формы и размера в электрическом поле;
- цементация, заключающаяся в восстановлении компонентов на металлах с отрицательными потенциалами;
- простая отгонка (выпаривание) — удаление веществ, находящихся в форме готовых летучих соединений;
- возгонка (сублимация) — перевод вещества из твердого состояния в газообразное и последующее осаждение его в твердой форме, минуя жидкую фазу;
- кристаллизация— образование зародышей твердой фазы при охлаждении газа, расплава или раствора.

Термические методы анализа используют термические эффекты, которые являются причиной или следствием химических реакций, и процессы выделения или поглощения теплоты в результате физических процессов.

В основе химических методов анализа лежат химические реакции трех типов: кислотно-основные, окислительно-восстановительные и комплексообразования. Основными из них являются классические гравиметрический и титриметрический методы. Гравиметрический метод заключается в выделении (путем осаждения, отгонки и т. Д.) в чистом виде вещества и его взвешивании. Методы, основанные на учете скорости химической реакции в зависимости от концентрации взаимодействующих веществ, представляют собой кинетические химические методы.

Электрохимические методы анализа изучают и используют процессы, протекающие не поверхности электрода и в приэлектродном пространстве. Различают прямые и косвенные электрохимические методы. В прямых методах используют связь между силой тока (величиной потенциала и т. Д.) и концентрацией определяемого вещества, в обратных — зависимость измеряемого электрического параметра от объема титрата (раствора с определенной концентрацией).

Хроматография — физико-химический метод разделения и анализа смесей, основанный на распределении их компонентов между подвижными и неподвижными веществами. Жидкость или газ (подвижное вещество) протекают мимо неподвижного твердого вещества или пленки жидкости, нанесенной на него. Хроматографические методы классифицируются по агрегатному состоянию смеси (газ, жидкость), по механизму разделения, по форме проведения хроматографического процесса (колоночная, капиллярная, плоскостная).

Спектральный анализ проводится с целью определения состава вещества по его спектру. Различают атомарный, молекулярный спектральный, эмиссионный (по спектрам излучения) и адсорбционный (по спектрам поглощения) методы анализа. В качественном анализе полученный спектр идентифицируют и интерпретируют с помощью таблиц и атласов спектров элементов и индивидуальных соединений. В количественном спектральном анализе определяют состав вещества по относительно или абсолютной интенсивностям полос спектра.

Масс-спектрометрические методы позволяют исследовать вещества путем определения масс и распределения частиц, содержащихся в веществе. С этой целью производится ионизация атомов и молекул изучаемого вещества и разделение образующихся ионов в пространстве или времени.

Методы анализа веществ, основанные на радиоактивности, разделяют на группы:
- радиоактивный анализ,
- радиоиндикаторные,
- основанные на поглощении и рассеянии радиоактивных излучений,
- радиометрические.

Наиболее распространен радиоактивный метод исследования радиоактивного

излучения нуклидов под воздействием потока элементарных частиц.

Биохимические методы используют биологические компоненты (ферменты, антитела и др.).

Если количество добытого вещества очень мало (порядка 100 мкг), то применяют микрохимический анализ, при меньшем количестве (единицы и доли мкг) — ***методы ультромикрохимического анализа.***

Простейшие методы качественного микрохимического анализа предусматривают получение в капле раствора на фарфоровой пластинке окрашенных продуктов реакции и выделение в капиллярных пробирках осадков, характерных для конкретного элемента. В качественном микрохимическом анализе наиболее универсальным методом является капельный анализ, для которого раствор и высокочувствительные реагенты берутся в количестве нескольких капель. Для обнаружения определенных ионов используют характерные цветные реакции, которые проводят на фильтровальной бумаге, часовом стекле, капельной пластинке, в микротигле. Полуколичественная капельная калориметрия выполняется путем сравнения интенсивности окраски пятен, полученных на фильтровальной бумаге, с окраской стандарта. Чувствительность этого метода составляет (0,01-0,1) мкг.

В количественном микроанализе используются гравиметрические, титрометрические, фотометрические методы. Титрометрические методы занимают ведущее положение как наиболее простые и высокоточные. Предпочтение отдается электрохимическим методам титрования, прежде всего кулометрическим.

Кулометрия — совокупность электрохимических методов анализа, основанных на измерении количества электричества, расходуемого при выделении на электроде того или иного вещества.

Весьма малые количества вещества исследуются методами ультрамикрохимического анализа. Приемы подготовки к анализу весьма специфичны и индивидуальные для каждого образца. Операции ультрамикрохимического анализа выполняются в капиллярной посуде через лупу и с помощью микроскопа с микроманипулятором. При наблюдении в микроскоп выполняют:

- осаждение в микроконусе с последующим отделением осадка центрифугированием;
- электролиз на микроэлектродах из тонкой проволоки;
- титрование в капиллярных ячейках;
- определение в виде окрашенных соединений в капиллярных кюветах с помощью микроскопов-фотометров.

В ультрамикрохимическом анализе органических веществ наряду с титрированием и спектрофотометрией применяют методы газовой хроматографии и газового анализа. Образцы для ультрамикрохимического анализа взвешивают на ультрамикровесах с точностью 10^{9}—10^{8} г. Проблемы анализа малых образцов обеспечиваются также сочетанием методов ультрамикрохимического исследования и физических методов.

1. 6 Лекция № 6 (2 часа).

Тема: «Способы и средства защиты информации от наблюдения и подслушивания»

1.6.1 Вопросы лекции:

1. Способы и средства противодействия наблюдению в оптическом диапазоне волн

1.6.2 Краткое содержание вопросов:

1. Способы и средства противодействия наблюдению в оптическом диапазоне волн

При защите информации от наблюдения в оптическом диапазоне необходимо учитывать факторы, влияющие на вероятность обнаружения (распознавания) объектов

наблюдения и ухудшающие точность измерения видовых демаскирующих признаков.

Эффективность поиска объектов наблюдения зависит от:

- яркости объекта;
- контраста объект/фон;
- угловых размеров объекта;
- угловых размеров поля обзора;
- времени наблюдения объекта;
- скорости движения объекта.

Яркость объекта на входе оптического приемника определяет мощность носителя, превышение которой над мощностью помех является необходимым условием получения изображения с необходимым качеством. Современные приемники имеют чувствительность, соответствующую энергии нескольких фотонов.

Контрастность объекта с окружающим фоном является необходимым условием выделения демаскирующих признаков объекта и его распознавания. Различают яркостной и цветовой контраст. Яркостной контраст $К_я$ определяют как отношение разности яркости объекта и фона к яркости объекта или фона:

$$К_я = (В_о - В_ф)/В_о,\ В_о > В_ф \quad \text{или} \quad К_в = (В_ф - В_о)/В_ф,\ В_ф > В_о,$$

где $В_о$ и $В_ф$ — яркость объекта и фона соответственно.

Относительная разность яркостей отдельных спектральных составляющих света от объекта и фона характеризует их **цветовойконтраст**. В видимом и ближнем диапазонах света яркостной контраст на входе оптической системы средства добывания несколько снижается за счет яркости дымки, которую можно рассматривать как помеху. В дальних зонах инфракрасного излучения яркостьдымки не оказывает существенного влияния на изменение этого контраста. Контраст может принимать значения в диапазоне 0-1. При $К_я$ = 0,08-0,1 объект почти сливается с фоном и плохо различается на фоне. Значения цветового контраста объектов и фона могут существенно отличаться в разных длинах волн, что используется в зональной (через цветовые фильтры) аэрофотосъемке.

При поиске объекта его форма не играет большой роли, а имеет значение только его площадь в пределах соотношения сторон от 1:1 до 1:10. Увеличение угловых**размеров** объекта в 2 раза сокращает время, необходимое для его обнаружения, в 8 раз.

Время для обнаружения объектов светлее и темнее фона при одинаковых абсолютных значениях контраста примерно одинаковое. С увеличением яркости фона время поиска объекта наблюдателем уменьшается, так как увеличивается разрешающая способность и контрастная чувствительность глаза. Если яркость фона чрезмерно велика, то возникают дискомфорт и ослепление, ухудшающие разрешение и контрастную чувствительность глаза.

С увеличением **поля обзора** увеличивается и время, необходимое для поиска объекта: двукратное увеличение поля обзора повышает время поиска в 4 раза. При этом время поиска определяется не формой поля, а его угловыми размерами.

Поиск движущихся объектов имеет свои особенности: движение ухудшает видимый контраст объекта, величина которого зависит не только от угловой скорости, но и от угловых размеров объекта наблюдения. Чем меньше угловой размер объекта, тем больше влияние **скорости** на время и вероятность обнаружения объекта. Объекты, движущиеся с малой скоростью, обнаруживаются легче,чем неподвижные, а движущиеся с большой скоростью — труднее из-за ухудшения видимого контраста.

Следовательно, в интересах защиты информации об объекте (его демаскирующих признаков) необходимо уменьшать контраст объект/фон, снижать яркость объекта и уменьшать угловые размеры объекта, не допуская наблюдателя близко к объекту.Мероприятия, направленные на уменьшение величины контраст/ фон, называются **маскировкой.**

С учетом этих факторов и общих методов инженерно-технической защиты информации методы защиты информации от наблюдения в оптическом диапазоне указаны на рис. 3.20.

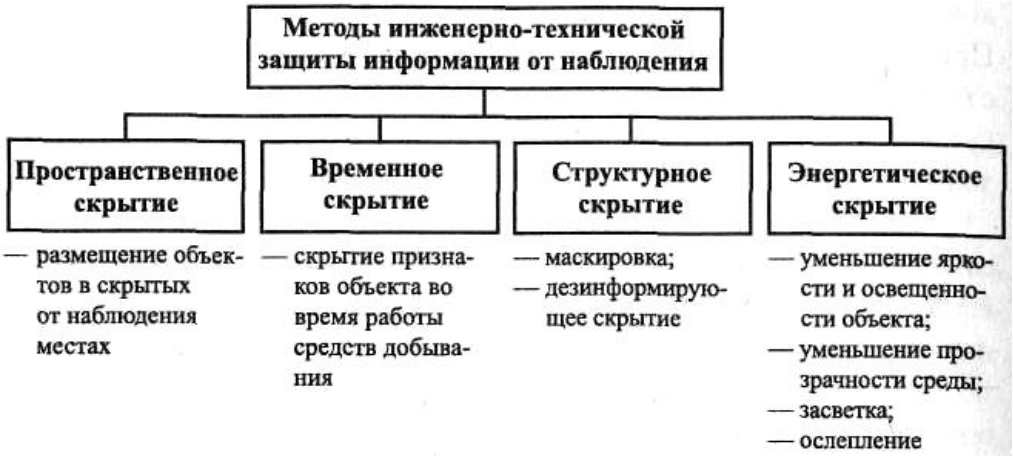


Рис. 3.20. Методы защиты информации от наблюдения

Пространственное скрытие обеспечивается размещением объектов защиты в точках (местах) пространства, неизвестных злоумышленнику или недоступных для наблюдения. С этой целью предприятия военно-промышленного комплекса размещали подальше от границ Советского Союза, а районы их нахождения объявлялись зонами, закрытыми для посещения иностранцами. Также для выделенных помещений в здании выбираются комнаты в отсеках с ограниченным допуском в них сотрудников.

Если время наблюдения известно, то достаточно эффективной мерой является перевод объекта наблюдения в состояние, в котором не проявляются видовые признаки в течение времени наблюдения. Например, при подлете разведывательного КА к полигону, на котором испытывается новая военная техника, работы, в ходе выполнения которых проявляются видовые демаскирующие признаки, прекращаются до момента выхода КА из зоны наблюдения.

Маскировка представляет собой метод структурного скрытия объекта защиты путем изменения его видовых признаков под признаки других объектов (фона). Применяются следующие способымаскировки:

- использование маскирующих свойств местности;
- маскировочная обработка местности;
- маскировочное окрашивание;
- применение искусственных масок;
- нанесение на объект воздушных пен.

¶Использование маскирующих свойств местности (неровностей ландшафта, складок местности, холмов, гор, стволов и кроны деревьев и т. д.) является наиболее дешевым способом скрытия объектов. Однако для реализации этого способа необходимо наличие в месте нахождения объекта соответствующих естественных масок.Кроме того, маскирующие возможности растительности зависят от времени года. Эффективность маскировки оценивается отношением площади, закрываемой, например, деревьями к площади наблюдаемой зоны.

Если отсутствуют или недостаточны для маскировки природные условия, то возможна дополнительная обработка местности, повышающая ее маскирующие возможности. Она состоит в дерновании (укладке дерна) и посеве травы, создании изгородей из живой растительности, в механической и химической обработке участков местности — распятнении. Обработка местности направлена на изменение фона под основной цвет объекта: на зеленый при дерновании и посеве травы или другой цвет (бурый с различными оттенками, соломенно-желтый) при распятнении.

Распятнение достигается расчисткой поверхности почвы от дерна с помощью машин или химическим путем — солями (железным и медным купоросом, бертолетовой

солью и др.) и гербицидами. Этот способ имеет ограниченное применение в связи с большой задержкой проявлений маскировочных свойств местности после обработки и вредным воздействием на природу. Например,трава вырастает через несколько недель после посева, а цвет растительности меняется через несколько дней после ее химической обработки.

Маскировочная обработка местности эффективна для скрытия наземных объектов и фона при наблюдении сверху, например, летного поля аэродрома для легких самолетов и вертолетов.

Маскировочное окрашивание применяется для изменения цвета объекта, маски или фона и производится путем:

- поверхностной окраски, при которой красочный слой наносится на окрашиваемую поверхность;
- глубинной окраски, при которой краситель пропитывает окрашиваемый материал (ткани, маскировочной сети) или вводятся пигменты при изготовлении материала (цветных цемента, штукатурки, пластмассы и др.).

При поверхностной окраске применяются различные краски, лаки, эмали, битумы, пасты, при глубинной окраске — синтетические красители, порошкообразные пигменты и крупнофракционные цветные материалы (песок, молотые руды).

Различают три вида маскировочного окрашивания:

- защитное;
- деформирующее;
- имитационное.

Защитное окрашивание поверхности объекта проводится одноцветной краской под цвет и среднюю яркость фона окружающей местности и предметов возле маскируемого объекта. Цвета защитного окрашивания: хаки, желтовато-серый, серо-зеленоватый, голубовато-серый, оливковый относятся к так называемым универсальным, которые плохо выделяются на фоне разнообразных объектов, прежде всего ландшафта. Однотонный желто-сероватый цвет полевого обмундирования солдат армий многих государств был плохо заметен на растительном, горном, пустынном, городском фонах. Приблизительно такими же возможностями обладал грязно-зеленовато-серый цвет немецкого обмундирования во Второй мировой войне. Защитная окраска оливкового или зеленовато-грязного цвета использовалась как заводская для военной техники.

Деформирующее окрашивание предусматривает нанесение на поверхность объекта пятен неправильной геометрической формы 2-3 цветов, имитирующих световые пятна окружающей среды. Различают мелкопятнистую (дробящую) и крупнопятнистую (искажающую контуры) деформирующую окраску. Края цветовых пятен могут быть резко очерченными или расплывчатыми. Деформирующее окрашивание психологически искажает образ защищаемого объекта у наблюдателя и затрудняет обнаружение и распознавание им объекта по признакам его формы. Оно в настоящее время является основным видом маскировки военнослужащих и военной техники армий большинства стран. Выпускается достаточно большое количество вариантов камуфляжа для разных времен года и типов местности. Наряду с маскировочными комбинезонами применяют маскировочные маски для лица или грим, которые наносят на лицо и руки и которые входит в состав маскировочного комплекта войск специального назначения. Деформирующая окраска труднее поддается дешифрованию на пестрых фонах и обеспечивает меньшую вероятность обнаружения и опознавания маскируемых объектов.

При **имитационном окрашивании** цвет и характер пятен на поверхности объекта подбираются под расцветку окружающей местности, объектов или предметов в месте расположения защищаемого объекта. Как правило, этот вид окрашивания применяется для неподвижных объектов: долговременных огневых сооружений, зданий, гидротехнических сооружений и др. В результате маскируемый объект сливается с окружающей местностью или приобретает внешний вид другого объекта. Например,

взлетно-посадочная полоса военного аэродрома может быть раскрашена под обычное шоссе или грунтовую дорогу с расположенными возле нее зданиями или иными объектами.

Маскировочное окрашивание просто реализуется, но эффект маскировки зависит от сезонных и иных изменений окружающей среды. Кроме того, частое перекрашивание объекта требует больших материальных и временных затрат.

Для маскировки без окрашивания создаются специальные конструкции — искусственные оптические маски, снижающие яркостной и цветовой контраст объекта защиты и фона.

Энергетическое скрытие демаскирующих признаков объектов достигается путем:

- уменьшения яркости источников света объекта или освещенности объекта внешними источниками;
- снижения прозрачности среды распространения света от объекта наблюдения до злоумышленника или его технического средства;
- засветки изображения объекта посторонними световыми лучами — помехами;
- ослепления зрительной системы наблюдателя или светоприемника.

Первые два метода относятся к пассивным и приводят к уменьшению уровня светового сигнала на входе оптического приемника. Так как его светочувствительные элементы имеют собственные шумы, то при уровне сигнала ниже собственных шумов обнаружение и распознавание его становятся невозможными.

К активным методам энергетического скрытия относятся **засветка изображения** или**ослепление светочувствительного приемника.** Засветка возникает, когда изображение помехи накладывается на изображение объекта и фона. При этом уменьшается контраст изображения по отношению к фону. Действительно, при условии, что $B_о > B_ф$контраст изображения с учетом яркости $B_п$, создаваемой на фотографии и экране монитора помехой, равен величине

$$K_{яп} = \frac{B_о + B_п - (B_ф + B_п)}{B_о + B_п} = \frac{B_о - B_ф}{B_о + B_п},$$

где $B_о$ и $B_ф$ — значение яркости объекта и фона соответственно. С увеличением мощности помехи (яркости $B_п$) контраст $K_{яп} \to 0$

Засветка происходит, когда солнечные лучи попадают на экран монитора компьютера или при наблюдении объектов через освещаемые светом стекла окон помещения или салона автомобиля. При наблюдении через стекло изображение формируется суммойлучей, отраженных от объектов наблюдения и от стекла. Свет от стекла представляет собой помеху. Световой поток от объекта наблюдения уменьшается стеклом, вследствие чего яркость помехи становится больше яркости объекта и фона. Эту разницу увеличивают применением тонированных (затемненных) или «зеркальных» (с алюминиевым или медным напылением) стекол. Тонированныестекла уменьшают $B_о$ и $B_ф$, а «зеркальные» увеличивают $B_п$. В результате этого контрастность объекта наблюдения уменьшается до величин, при которых объект на виден.

При превышении мощности помехи на входе приемника значения, соответствующего его динамическому диапазону, возникают искажения информации вплоть до ее полного разрушения. Чрезмерно большая мощность помехи может привести к необратимым изменениям в светочувствительных элементах. Например, высокочувствительные телевизионные камеры, позволяющие наблюдать за обстановкой при очень малом освещении, могут выйти из строя при попадании на ПЗС-матрицу прямых лучей солнечного света.

Классическим примером ослепления может служить применение наступающими советскими войсками ночью в Берлинской операции 1945 г. 142 прожекторов, свет которых лишил фашистов возможности видеть наступающие войска и эффективно обороняться. Наиболее естественным способом энергетического скрытия является проведение мероприятий, требующих защиты информации о них, ночью. Яркость

объектов, имеющих искусственные источники света, снижается путем их выключения или экранирования светонепроницаемыми шторами и экранами.

Энергетическое скрытие объектов, наблюдаемых в отраженном свете, обеспечивают естественные и искусственные маски, а также аэрозоли в среде распространения.

Так как спектральные характеристики объектов и среды различаются для видимого и ИК-диапазонов, то при организации защиты информации от наблюдения в оптическом канале необходимоучитывать диапазон частот носителя информации. Хотя параметры средств визуально-оптического наблюдения (по разрешению,дальности, цвету изображения) в ИК-диапазоне значительно более низкие чем в видимом, но при наблюдении в нем появляется дополнительный демаскирующий признак объектов, не обнаруживаемый в видимом, — температура поверхности объекта относительно температуры фона.

Естественный фон в ИК-диапазоне можно рассматривать как сложный источник ИК-излучения, характеристики которого зависят от условий освещения, географической широты и долготы, сезона и температуры среды, метеоусловий, природы подстилающей поверхности, времени года и дня и т. п. Отражающая способность ряда природных фонов, таких как трава и листва деревьев, возрастает со смещением максимума излучений в область более длинных волн. Например, отражающая способность травы и листвы в диапазоне волн 0,76-12 мкм выше отражающей способности в видимомдиапазоне приблизительно в 5-10 раз, коры — в 3-5 раз. Поэтому объекты, окрашенные маскирующей краской для видимого диапазона, могут хорошо наблюдаться в ИК-диапазоне. Следовательно, при выборе краски необходимо учитывать характер изменения ее коэффициента отражения от длины волны падающего на объект света, в том числе и в ИК-диапазоне.

Основными средствами скрытия объектов наблюдения в оптическом диапазоне являются краски, различные маски и экраны. При выборе красок для маскировочного окрашивания кроме цвета важно учитывать характер изменения коэффициента отражения от длины волны. Чем меньше отличаются коэффициенты отражения краски в видимом и инфракрасном диапазонах волн, тем лучше ее маскирующая способность.

Искусственные оптические маскировочные маски в зависимости от ее формы и способа расположения возле объекта делятся на следующие типы:

- маски-навесы;
- вертикальные маски;
- маски перекрытия;
- наклонные маски;
- радиопрозрачные маски.

Маски-навесы предназначены для скрытия объектов, расположенных на открытых сверху площадках и защищают их от наблюдения с помощью средств, размещаемых на верхних этажах высотных зданий, возвышенностях и горах, на самолетах и космических аппаратах.

Вертикальные маски защищают объекты от наблюдения **с** земли. Маски перекрытия состоят из каркаса и маскировочного покрытия, которые полностью закрывают объект. Они применяются, прежде всего, для защиты объектов, перевозимых на открытых платформах.

Наклонные маски используются в основном для скрытия теней объемных объектов, по длине которых с учетом положения солнца определяют высоту объектов при наблюдении сверху (с самолетов и космических аппаратов).

Радиопрозрачные маски выполняются из радиопрозрачныхматериалов (стеклопластика, пенопласта и др.), обычно в форме шара, для скрытия демаскирующих признаков и физической защиты антенн.

Искусственные оптические маски изготовляются из подручных материалов (хвороста, камыша, тростника, кустарника) или из табельных средств и материалов (маскировочной сети, устойчивой к воздействию факторов погоды, армированной маскировочной бумаги, сетчатой ткани, полихлорвиниловой пленки и др.), а также ввиде различных сборных возимых маскировочных комплектов.

Для маскировки военной техники в оптическом диапазоне используются различные типы **табельных маскировочных комплектов (МКТ):** МКТ-Л — для маскировки на растительном фоне или обнаженном грунте, МКТ-С — для снежных фонов, МКТ-П — для горно-пустынной местности, МКТ-Т — для маскировки танков и др. Комплект представляет собой металлический разборныйкаркас, на который натягивается окрашенная в различные цвета специальная сплошная или сетчатая ткань с двусторонней окраской для разных фонов. Маскировочное покрытие одного комплекта имеет максимальный размер $12^{x}18$ м (из расчета создания маски для танка) и состоит из 12 фрагментов размером $3^{x}6$ м каждый. Фрагменты соединяются между собой сшивными шнурами, которые позволяют оперативно собирать покрытия различной конфигурации и размера, в том числе плоские, выпуклые, вертикальные, наклонные, маски-макеты, маски-навесы. С помощью запасных сшивных шнуров, входящих в маскировочный комплект, можно объединять покрытия несколько комплектов для укрытия крупных объектов.

Искусственные оптические маски могут применяться многократно, не оказывают вредное воздействие на природу, совместимы с другими способами защиты.

Светонепроницаемые одно- и **многоцветные воздушные пены,** быстро наносимые с помощью генераторов пены на объекты, обеспечивают их эффективную маскировку в широком диапазоне длин волн в течение до нескольких часов.

Маски, которые создают у наблюдателя представление о другом объекте (объекте прикрытия), называются **деформирующими.**Например, при перевозке орудий на железнодорожных платформах их скрывают под брезентом, которым накрывают деревянный прямоугольный каркас. Наблюдатель по факту присутствия часовых на платформе сделает вывод о перевозке военной техники, но определить вид перевозимой техники не сможет. Во время битвы за Москву с помощью деформирующих масок и имитационного окрашивания для дезинформирования немецких летчиков мавзолей Ленина имел сверху вид двухэтажного особняка, а кремлевские башни были похожи на водонапорные башни и высотные здания.

Для дезинформирующего скрытия применяются кроме деформирующих масок **ложные сооружения** и **конструкции,** создающие признаки ложного объекта (объекта прикрытия). Ложные сооружения могут быть плоскими и объемными, функциональными и нефункциональными. Они относятся к наиболее дорогим средствам защиты информации, особенно объемные и функциональные, так как должны воспроизводить полный набор демаскирующих признаков объекта прикрытия в динамике в течение всего периода защиты. Если, например, имитируется объект, на котором работают люди, то они должны убедительно изображать соответствующую деятельность, а не устраивать непрерывные перекуры или греться на солнышке.

Энергетическое скрытие демаскирующих признаков объектов достигается путем уменьшения яркости объекта и фона ниже чувствительности глаза или технического фотоприемника, а также их ослепления. Наиболее естественным способом энергетического скрытия является проведение мероприятий, требующих защиты информации о них, ночью. Яркость объектов, имеющих искусственные источники света, снижается путем их выключения или экранирования светонепроницаемыми шторами и экранами.

Для экранирования объектов наблюдения в помещении применяются шторы, занавески, жалюзи, тонированные стекла и пленки. Эффективные экраны создают жалюзи. По виду материалов жалюзи делятся на тканевые, пластиковые, деревянные и металлические. Лучшие эксплуатационные свойства имеют деревянные и металлические

жалюзи. По расположению ламелей жалюзи бывают вертикальные, горизонтальные и рулонные.

Энергетическое скрытие объектов, наблюдаемых в отраженном свете, обеспечивают рассмотренные искусственные маски, а также естественные и искусственные аэрозоли в среде распространения.

Аэрозоли — вещества в виде дисперсии твердых частиц и капель жидкости, находящихся во взвешенном состоянии в воздухе. К аэрозолям относятся обычно дымы, туманы, пыль, смог.

Естественные аэрозоли образуются обычно пылью и частицами воды. В зависимости от размеров частиц воды метеорологическая дальность изменяется от десятков метров (при очень сильном тумане, дожде и снеге) до 10-20 км (при дымке). Хорошая видимость обеспечивается при дальности 20-50 км, а исключительно хорошая — более 50 км.

Наиболее распространенной разновидностью аэрозольного состояния атмосферы является дымка. Дымка возникает при слипании мелкодисперсных частиц воздуха друг с другом и взаимодействии их с атмосферной влагой. В условиях повышенной влажности воздуха в результате взаимодействия паров воды с частицами растворимых в ней солей образуется туманная дымка, при которой метеорологическая дальность составляет 1-10 км.

Влияние аэрозольных образований в общем случае проявляется как в рассеянии, так и поглощении света частицами аэрозоля.Коэффициент ослабления (поглощения) в видимой области спектра изменяется в 1,5-2 раза. С увеличением длины волны потери ослабевают. Потери энергии волны приλ= 0,55 мкм приблизительно в 10 раз больше потерь дляλ= 1,06 мкм. Аэрозольное рассеяние света зависит от коэффициентов его ослабления отдельными частицами, их концентрации и размеров. Оно определяет прозрачность и метеорологическую дальность видимости.

Использование естественных аэрозолей в качестве средств защиты от наблюдения затруднено из-за случайного характера их проявлений в виде образований, приводящих к малой метеорологической дальности. Тем не менее естественные аэрозоли в виде облаков создают серьезные проблемы для разведки при наблюдении наземных и надводных объектов с помощью средств космической разведки. Учитывая, что траектории движения КА и облаков независимые, вероятность выполнения временного условия разведывательного контакта (совпадения моментов пролета спутника над интересующим разведку объектом и отсутствием облачности) равна произведению вероятностей каждого из этих событий. Следовательно, для обнаружения и распознавания объекта даже при отсутствии мер защиты информации о нем потребуютсямногократные пролеты над ним разведывательных КА.

С помощью дымовых шашек, специальных боеприпасов (снарядов, бомб), аэрозольных генераторов и дымовых машин создаются дымовые завесы (облака) из искусственных аэрозолей, обеспечивающих (при учете направления и силы ветра) эффективное, но кратковременное скрытие. Время и площадь скрытия зависят от многих факторов, в том числе от объема облака дыма, направления и скорости ветра, и колеблется от минут до 1-2 часов. Наиболее эффективные завесы образуются при скорости ветра 3-5 м/с.

В качестве химических веществ для образования дыма применяются эпоксидные, фенольные, полиэтиленовые, силикатные,уретановые смолы и другие высокомолекулярные соединения. Дымы из таких веществ получаются разделением частиц веществав потоке горячих газов и другими способами. В зависимости от состава компонентов частицы, образующие аэрозольное облако, могут иметь диаметр от 1 до 100 мкм. Для образования аэрозольного облака, обеспечивающего, например, ослабление излучений в ИК-диапазоне примерно в 80 раз, на площади 600 м^{2}потребуется распылить около 400 г дымообразующего вещества.

Кроме того, на яркость объекта с собственными источниками тепла, и, следовательно, на его контраст с фоном в ИК-диапазоне влияет температура поверхности объекта. Для защиты объектов от наблюдения в инфракрасном диапазоне применяются различные теплоизолирующие экраны, в том числе подручные материалы с плохой теплопроводностью: листья деревьев и кустарников, сено, брезент и др. Хорошими теплоизолирующими свойствами обладают воздушные пены.

Так как скрытое наблюдение проводится, как правило, с помощью оптических приборов, то для противодействия наблюдению применяются активные средства обнаружения оптики. Такиесредства представляют собой приборы ночного видения с лазерной подсветкой. Средство содержит лазерный излучатель в инфракрасном диапазоне длин волн, лучи которого сканируют наблюдаемоепространство. Отраженный от поверхности линзы объектива луч лазера обозначает место нахождения оптического прибора точкой повышенной яркости на изображении.

1. 7 Лекция № 7 (2 часа).

Тема: «Способы и средства защиты информации, обрабатываемой средствами вычислительной техники**»**

1.7.1 Вопросы лекции:

1. Общая характеристика технических каналов утечки информации, обрабатываемой средствами вычислительной техники.
2. Электромагнитные каналы утечки информации, обрабатываемой средствами вычислительной техники

1.7.2 Краткое содержание вопросов:

1. Общая характеристика технических каналов утечки информации, обрабатываемой средствами вычислительной техники.

Для обработки информации ограничен-ного доступа широко используются различ-ные информационные системы, основу ко-торых составляют средства вычислительной техники (СВТ). Поэтому объекты информа-тизации, на которых обработка информации осуществляется с использованием СВТ, часто называются «объектами СВТ».

При рассмотрении объекта СВТ, как объекта защиты от утечки информации по техническим каналам, его необходимо рас-сматривать как объект, включающий:

- технические средства и системы, непосред-ственно обрабатывающие информацию ограниченного доступа, вместе с их соеди-нительными линиями (под соединительны-ми линиями понимают совокупность про-водов и кабелей, прокладываемых между отдельными ТСОИ и их элементами);
- вспомогательные технические средства и си-стемы вместе с их соединительными линиями;
- посторонние проводники;
- систему электропитания;
- систему заземления.

К техническим средствам обработки информации ограниченного доступа (ТСОИ) относятся:

- технические средства автоматизированных систем управления, электронно-вычислительные машины и их отдельные элементы, в дальнейшем именуемые средствами вычислительной техники (СВТ);
- средства изготовления и размножения документов;
- аппаратура звукоусиления, звукозаписи, звуковоспроизведения и синхронного перевода;
- системы внутреннего телевидения;
- системы видеозаписи и видеовоспроизведения;

- системы оперативно-командной связи;
- системы внутренней автоматической телефонной связи, включая и соединительные линии перечисленного выше оборудования и т.д.

Данные технические средства и системы в ряде случаев именуются основными техническими средствами и системами (ОТСС).

Наряду с техническими средствами и системами, обрабатывающими информацию ограниченного доступа, в помещениях, где они установлены, как правило, находятся и другие технические средства и системы, которые в обработке информации ограниченного доступа непосредственно не участвуют. К ним относятся:

- системы и средства городской автоматической телефонной связи;
- системы и средства передачи данных в системе радиосвязи;
- системы и средства охранной и пожарной сигнализации;
- системы и средства оповещения и сигнализации;
- контрольно-измерительная аппаратура;
- системы и средства кондиционирования;
- системы и средства проводной радиотрансляционной сети и приёма программ радиовещания и телевидения (абонентские громкоговорители, средства радиовещания;
- телевизоры и радиоприёмники и т.д.);
- средства электронной оргтехники;
- системы и средства электрочасофикации и иные технические средства и системы. **Такие технические средства и системы называются вспомогательными техническими средствами и системами (ВТСС)**

Через помещения, в которых установлены технические средства обработки информации ограниченного доступа, могут проходить провода и кабели, не относящиеся к ТСОИ и ВТСС, а также металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции, которые называются **посторонними проводниками (ПП).**

Электропитание ТСОИ и ВТСС осуществляется от распределительных устройств и силовых щитов, которые специальными кабелями соединяются с трансформаторной подстанцией городской электросети.

Все технические средства и системы, питающиеся от электросети, должны быть заземлены. Типовая система заземления включает общий заземлитель, заземляющий кабель, шины и провода, соединяющие заземлитель с техническими средствами.

Ряд соединительных линий ВТСС, посторонних проводников, а также линии электропитания и заземления могут выходить за пределы **контролируемой зоны** объекта (КЗ), под которой понимается пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание посторонних лиц (посетителей, работников различных технических служб, не являющихся сотрудниками организации), а также транспортных средств. Границей контролируемой зоны могут являться периметр охраняемой территории организации, а также ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории.

Совокупность информационных ресурсов, содержащих сведения ограниченного доступа, технических средств и систем обработки информации ограниченного доступа, вспомогательных технических средств и систем, помещений или объектов (зданий, сооружений), в которых они установлены, составляет **защищаемый объект информатизации (ОИ).**

Защищаемые объекты информатизации **должны аттестовываться по требованиям безопасности информации.**

Помещения, предназначенные для ведения закрытых переговоров, содержащих сведения, отнесённые к государственной тайне, называются **выделенными помещениями (ВП),** а помещения, предназначенные для ведения конфиденциальных переговоров - **защищаемыми помещениями (ЗП).**

Выделенные и защищаемые помещения также должны **аттестовываться по требованиям безопасности информации**

Иностранные разведки для перехвата информации используют **технические средства разведки (ТСР).**

Для перехвата информации, обрабатываемой СВТ, используются **технические средства разведки побочных электромагнитных излучений и наводок (ТСР ПЭМИН).**

Другие заинтересованные субъекты (юридические лица, группы физических лиц, отдельные физические лица) для перехвата информации используют **специальные технические средства (СТС), приспособленные или доработанные для негласного получения информации.**

В зависимости от природы образования информативного сигнала технические каналы утечки информации можно разделить на естественные и специально создаваемые .

Естественные каналы утечки информации образуются за счёт побочных электромагнитных излучений, возникающих при обработке информации СВТ (электромагнитные каналы утечки информации), а также вследствие наводок информативных сигналов в линиях электропитания СВТ, соединительных линиях ВТСС и посторонних проводниках (электрические каналы утечки информации).

К **специально создаваемым каналам утечки информации** относятся каналы, создаваемые путём внедрения в СВТ электронных устройств перехвата информации (закладных устройств) и путём «высокочастотного облучения» СВТ.

2. Электромагнитные каналы утечки информации, обрабатываемой средствами вычислительной техники

В электромагнитных каналах утечки информации носителем информации являются электромагнитные излучения (ЭМИ), возникающие при обработке информации техническими средствами.

Основными причинами возникновения электромагнитных каналов утечки информации в ТСОИ являются:

- побочные электромагнитные излучения, возникающие вследствие протекания информативных сигналов по элементам ТСОИ;
- модуляция информативным сигналом побочных электромагнитных излучений высокочастотных генераторов ТСОИ (на частотах работы высокочастотных генераторов);
- модуляция информативным сигналом паразитного электромагнитного излучения ТСОИ (например, возникающего вследствие самовозбуждения усилителей низкой частоты).

Побочные электромагнитные излучения (ПЭМИ) – нежелательные (паразитные) электромагнитные излучения, возникающие при функционировании технических средств обработки информации, и приводящие к утечке обрабатываемой информации.

С точки зрения защиты информации опасность представляют информативные ПЭМИ, содержащие в себе признаки обрабатываемой информации.

Информативными ПЭМИ называются сигналы, представляющие собой ВЧ несущую, модулированную информацией обрабатываемой на СВТ (например, изображением выводимым на монитор, данными обрабатываемыми на устройствах ввода-вывода и т.д.).

Неинформативными ПЭМИ называются сигналы, анализ которых может дать представление только о режиме работы СВТ и никак не раскрывает характер информации, обрабатываемой на СВТ.

Диапазон возможных частот ПЭМИ зависит от типа СВТ и может составлять от сотен Гц до десятков ГГц.

Побочные электромагнитные излучения возникают при следующих режимах обработки информации средствами вычислительной техники:

- вывод информации на экран монитора;
- ввод данных с клавиатуры;
- запись информации на накопители;
- чтение информации с накопителей;
- передача данных в каналы связи;
- вывод данных на периферийные печатные устройства - принтеры, плоттеры;
- запись данных от сканера на магнитный носитель и т.д.

Для перехвата побочных электромагнитных излучений СВТ используются специальные стационарные, перевозимые и переносимые приёмные устройства, которые называются техническими средствами разведки побочных электромагнитных излучений и наводок (ТСР ПЭМИН).

Типовой комплекс разведки ПЭМИ включает: специальное приёмное устройство, ПЭВМ (или монитор), специальное программное обеспечение и широкодиапазонную направленную антенну.

Наиболее опасным (с точки зрения утечки информации) режимом работы СВТ является вывод информации на экран монитора. Учитывая широкий спектр ПЭМИ видеосистемы СВТ ($\Delta Fc > 100$ МГц) и их незначительный уровень, перехват изображений, выводимых на экран монитора ПЭВМ, является довольно трудной задачей.

Дальность перехвата ПЭМИ современных СВТ, как правило, не превышает 30-50 м.

Качество перехваченного изображения значительно хуже качества изображения, выводимого на экран монитора ПЭВМ

В качестве показателя оценки эффективности защиты информации от утечки по техническим каналам используется вероятность правильного обнаружения информативного сигнала (P_0) приёмным устройством средства разведки. В качестве критерия обнаружения наиболее часто используется критерий «Неймана-Пирсона». В зависимости от решаемой задачи защиты информации пороговое значение вероятности обнаружения информативного сигнала может составлять от 0,1 до 0,8, полученное при вероятности ложной тревоги от 10^{-3} до 10^{-5}.

Зная характеристики приёмного устройства и антенной системы средства разведки, можно рассчитать допустимое (нормированное) значение напряжённости электромагнитного поля, при котором вероятность обнаружения сигнала приёмным устройством средства разведки будет равна некоторому (нормированному) значению ($P_0 = P_П$).

Пространство вокруг ТСОИ, на границе и за пределами которого напряжённость электрической (Е) или магнитной (Н) составляющей электромагнитного поля не превышает допустимого (нормированного) значения ($E \le E_n$; $H \le H_n$, называется опасной зоной 2 (R2).

Зона R2 для каждого СВТ определяется инструментально-расчётным методом при проведении специальных исследований СВТ на ПЭМИ и указывается в предписании на их эксплуатацию или сертификате соответствия.

Таким образом, для возникновения электромагнитного канала утечки информации необходимо выполнение двух условий:

- первое - расстояние от СВТ до границы контролируемой зоны должно быть менее зоны R2 R < R2);
- второе - в пределах зоны R2 возможно размещение стационарных или перевозимых (переносимых) средств разведки ПЭМИН.

1. 8 Лекция № 8 (2 часа).

Тема: «Системный подход к инженерно-технической защите информации»

1.8.1 Вопросы лекции:

1. Правовая основа системы лицензирования, сертификации и аттестации объектов информатизации в Российской Федерации
2. Лицензирование деятельности по защите информации
3. Сертификация средств защиты информации
4. Аттестация объектов информатизации

1.8.2 Краткое содержание вопросов:

1. Правовая основа системы лицензирования, сертификации и аттестации объектов информатизации в Российской Федерации

Система обеспечения государственной безопасности базируется на своде законов и нормативно правовых документов РФ по лицензированию деятельности в сфере защиты информации, сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации.

Органы государственной власти субъектов Российской Федерации и органы местного самоуправления в своей деятельности используют все виды государственной тайны и информацию, относимую в соответствии с законодательством Российской Федерации к конфиденциальной. Для того чтобы законно хранить и использовать секретную и конфиденциальную информацию органы власти должны иметь лицензии на проведение работ со сведениями соответствующей степени секретности, сертифицированные средства защиты информации и аттестованные объекты информатизации по требованиям безопасности информации.

Лицензия – выдаваемое уполномоченным лицом (лицензиаром) юридическим и физическим лицам (лицензиатам) разрешение на совершение определенных действий, без которого совершение таких действий признается неправомерным.

Лицензирование – это процесс, осуществляемый в отношении таких категорий, как «деятельность» (виды деятельности) и «субъект» (физическое лицо, предприятие, организация или иное юридическое лицо), когда некоторый субъект в результате проведения комплекса мероприятий, состав, правила и порядок осуществления которых предписываются законодательными и нормативными актами, получает право на ведение определенного вида деятельности. Это право закрепляется и оформляется в виде официальных документов, виды и статус которых также предписываются нормативными актами. За органом, уполномоченным на проведение лицензионной деятельности, закрепляется право на контроль за деятельностью лицензиата. Получить право на осуществление деятельности, подлежащей лицензированию, может не каждый, а лишь субъект, отвечающий определенным критериям, которые заранее определяются правилами проведения лицензирования и требованиями к предприятию-заявителю.

Таким образом, субъектом лицензирования становится лишь то физическое или юридическое лицо, которое представляет все необходимые и правильно оформленные документы и удовлетворяет соответствующим критериям.

Сертификат на средство защиты информации – документ, подтверждающий соответствие средства защиты информации требованиям по безопасности информации.

Система аттестации объектов информатизации по требованиям безопасности информации (далее - система аттестации) является составной частью единой системы сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации и подлежит государственной регистрации в

установленном Госстандартом России порядке.

Деятельность системы аттестации организует федеральный орган по сертификации продукции и аттестации объектов информатизации по требованиям безопасности информации, которым является ФСТЭК России.

Законодательной и нормативной базой лицензирования и сертификации в области ***защиты государственной тайны*** являются следующие документы:

– Закон Российской Федерации 1993 г. № 5485-1 «**О государственной тайне»;**

– Указ Президента Российской Федерации 1999 г. № 212 **«Вопросы государственной технической комиссии при Президенте Российской Федерации»;**

– Постановление Правительства Российской Федерации 1995 г. № 333 **«О лицензировании деятельности предприятий и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны»;**

– **Положение по аттестации объектов информатизации по требованиям безопасности информации 1994 г.;**

Законодательная база лицензирования в области защиты ***конфиденциальной информации*** включает:

– Закон Российской Федерации от 8.08.2001 г. № 128-ФЗ **«О лицензировании отдельных видов деятельности»;**

– Постановление Правительства Российской Федерации от 11.02.2002 г. № 135 **«О лицензировании отдельных видов деятельности»;**

– Постановление Правительства Российской Федерации от 30.04.2002 г. № 290 **«О лицензировании деятельности по технической защите конфиденциальной информации»;**

– Постановление Правительства Российской Федерации от 27.05.2002 г. № 348 **«Об утверждении Положения о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации»;**

Полный перечень видов деятельности в области защиты информации, подлежащих обязательному государственному лицензированию, определён в законах Российской Федерации «О государственной тайне» и «О лицензировании отдельных видов деятельности». В законе Российской Федерации "О государственной тайне" определены лицензируемые виды деятельности в области защиты информации, содержащей сведения, отнесённые к государственной тайне, а в законе Российской Федерации "О лицензировании отдельных видов деятельности" – в области защиты конфиденциальной информации.

2. Лицензирование деятельности по защите информации

Общие нормы, устанавливающие порядок допуска организаций к проведению работ с информацией, составляющей государственную тайну, содержатся в статье 27 закона Российской Федерации "О государственной тайне":

1. Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны, осуществляется путем получения ими в порядке, устанавливаемом Правительством Российской Федерации, лицензий на проведение работ со сведениями соответствующей степени секретности.

2. Лицензия на проведение указанных работ выдается на основании результатов специальной экспертизы предприятия, учреждения и организации и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих государственную тайну, расходы по проведению которых относятся на счет предприятия, учреждения, организации, получающих лицензию.

3. Лицензия на проведение работ с использованием сведений, составляющих государственную тайну, выдается предприятию, учреждению, организации при выполнении ими следующих условий:

– выполнение требований нормативных документов, утверждаемых Правительством Российской Федерации, по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ, связанных с использованием указанных сведений;

– наличие в их структуре подразделений по защите государственной тайны и специально подготовленных сотрудников для работы по защите информации, количество и уровень квалификации которых достаточны для обеспечения защиты государственной тайны;

– наличие у них сертифицированных средств и систем защиты информации.

Органами, уполномоченными на ведение лицензионной деятельности, являются:

1. В сфере допуска предприятий к проведению работ, связанных с использованием сведений, составляющих государственную тайну, – Федеральная служба безопасности Российской Федерации и ее территориальные органы (на территории Российской Федерации), Служба внешней разведки Российской Федерации (за рубежом).

2. В области лицензирования на право проведения работ, связанных с созданием средств защиты информации, – Федеральная служба по техническому и экспертному контролю, Федеральная служба безопасности.

3. В области лицензирования на право осуществления мероприятий и (или) оказания услуг в области защиты государственной тайны – Федеральная служба безопасности Российской Федерации и ее территориальные органы, Федеральная служба охраны (ФСО) и Служба внешней разведки РФ.

4. В сфере допуска предприятий к проведению работ, связанных с использованием конфиденциальной тайны, – органы, аккредитованные ФСТЭК России. Согласно статье 17 закона РФ “О лицензировании отдельных видов деятельности”, при работе с конфиденциальной информацией **лицензированию подлежат следующие виды деятельности:**

– деятельность по распространению шифровальных (криптографических) средств защиты информации;

– деятельность по техническому обслуживанию шифровальных (криптографических) средств защиты информации;

– предоставление услуг в области шифрования информации;

– деятельность по технической защите конфиденциальной информации.

Срок действия лицензии устанавливается в зависимости от специфики вида деятельности, но не может быть менее пяти лет. Продление срока действия лицензии производится в порядке, установленном для ее получения. На каждый вид деятельности выдается отдельная лицензия. Система лицензирования построена на следующих основных принципах:

1. Лицензирование в области защиты информации является обязательным.

2. Деятельность в области защиты информации физических и юридических лиц, не прошедших лицензирование, запрещена.

3. Лицензии на право деятельности в области защиты информации выдаются только юридическим лицам независимо от организационно – правовой формы, так как физические лица не в состоянии удовлетворить установленным требованиям.

4. Лицензии выдаются только предприятиям, зарегистрированным на территории Российской Федерации.

5. Лицензии выдаются только на основании специальной экспертизы заявителя на соответствие предъявляемым к предприятию требованиям и аттестации руководителя предприятия.

6. Для получения лицензии предприятие обязано предъявить определенный перечень документов.

К заявлению на получение лицензии необходимо приложить следующие документы (рис. 3.2.):

- копию свидетельства о государственной регистрации предприятия;
- копии учредительных документов, заверенных нотариусом;
- копии документов на право собственности или аренды имущества,
- необходимого для ведения заявленной деятельности;
- справка налогового органа о постановке на учет;
- документ, подтверждающий оплату лицензионного сбора;
- сведения о квалификации работников лицензиата.

Проведение экспертизы осуществляется экспертными комиссиями Лицензионного центра.

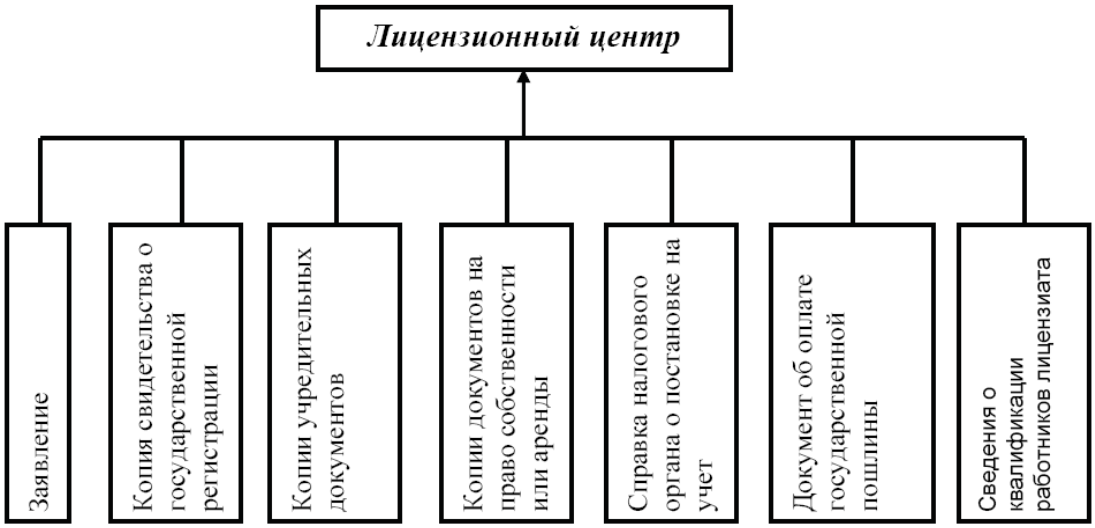


Рис. 1.3 Перечень документов, необходимых для получения лицензии

Организация несет ответственность за достоверность представленных сведений. Орган, выдающий лицензию, вправе проверить достоверность представляемых сведений.

Оформление лицензии и ее выдача (уведомление об отказе в выдаче) производится в тридцатидневный срок со дня подачи заявления со всеми необходимыми документами.

Основанием для отказа в выдаче лицензии является:

– наличие в документах, представленных заявителем, недостоверной или искаженной информации;

– отрицательное заключение экспертизы, установившей несоответствие необходимым для осуществления заявленного вида деятельности условиям;

– отрицательное заключение по результатам государственной аттестации руководителя предприятия.

Для рассмотрения спорных вопросов, возникающих при экспертизе предприятия-заявителя, может проводиться дополнительная независимая экспертиза. Состав экспертной комиссии формируется государственным органом по лицензированию по согласованию с предприятием-заявителем. Заключение экспертной комиссии является определяющим для принятия соответствующего решения в связи с заявлением о выдаче лицензии.

Время, затраченное на экспертизу, в срок, установленный для выдачи лицензии, не включается. Финансирование издержек за проведение дополнительной независимой

экспертизы несет сторона, признанная виновной в конфликте.

Действия органов, осуществляющих лицензирование, могут быть обжалованы в судебных органах в установленном порядке.

Органы, уполномоченные на ведение лицензионной деятельности, приостанавливают действие лицензии или ***аннулируют*** ее в случаях:

– представления лицензиатом соответствующего заявления;

– ликвидации юридического лица;

– обнаружения недостоверных данных в документах, представленных для получения лицензии;

– нарушения лицензиатом условий действия лицензии;

– использования лицензии для рекламирования не предусмотренных в ней видов деятельности;

– нарушения лицензиатом законодательства Российской Федерации, требований соблюдения налоговой дисциплины и соответствующих нормативных документов;

– невыполнения лицензиатом предписаний и распоряжений государственных органов или приостановление ими деятельности предприятия в соответствии с законами Российской Федерации.

В случае приостановления действия лицензии или ее аннулирования лицензиат информируется в письменном виде органом, выдавшим лицензию, не позднее пяти дней со дня принятия решения. В десятидневный срок после получения уведомления владелец лицензии обязан сдать ее в орган, выдавший лицензию.

Учет лицензиатов ведется государственными органами по лицензированию на основании сведений, поступающих от лицензионных центров.

Контроль и надзор за полнотой и качеством проводимых лицензиатами работ осуществляется при контроле государственными органами по лицензированию, лицензионными центрами качества выполненных лицензиатами работ по рекламациям предприятийпотребителей.

3. Сертификация средств защиты информации

Одним из обязательных условий получения лицензии на работу с государственной тайной является наличие в организации сертифицированных средств защиты информации.

Сертификация средств защиты информации, прежде всего, подразумевает проверку их качественных характеристик для реализации основной функции – защиты информации на основании государственных стандартов и требований по безопасности информации. Применительно к сведениям, составляющим государственную тайну, общие принципы организации сертификации средств защиты информации определены нормами статьи 28 Закона РФ "О государственной тайне" – средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности. Организация сертификации средств защиты информации возлагается на Федеральное агентство контроля экспорта и технологий, Министерство обороны РФ в соответствии с функциями, возложенными на них законодательством Российской Федерации. Сертификация осуществляется на основании требований государственных стандартов Российской Федерации и иных нормативных документов, утверждаемых Правительством России. Одним из основных руководящих документов по сертификации защиты информации в настоящее время является “Положение о сертификации средств защиты информации”, утвержденное Постановлением Правительства Российской Федерации от 25.06.95 г. № 608, реализующим нормы закона РФ "О сертификации продукции и услуг".

Порядок проведения сертификации основан на следующих принципах:

1.Обязанность сертификации изделий, обеспечивающих защиту государственной тайны.

2.Обязательность использования криптографических алгоритмов, являющихся

стандартами.

3. Принятие на сертификацию только изделий от заявителей, имеющих лицензию.

Таким образом, в соответствии с названными документами разработаны и введены в действие перечни средств защиты информации, подлежащих обязательной сертификации; государственным организациям и предприятиям запрещено использование в информационных системах шифровальных средств (в т.ч. электронной подписи и защищенных технических средств хранения, обработки и передачи информации), не имеющих сертификата.

Осуществляется следующий порядок сертификации:

1. В Центральный орган по сертификации (орган, аккредитованный ФСТЭК России) подается заявление и полный комплект технической документации.

2.Центральный орган назначает испытательный центр (лабораторию) для проведения испытания.

3. Испытания проводятся на основании хозяйственного договора между заявителем и испытательным центром.

4. Сертификация (экспертиза материалов и подготовка документов для выдачи) осуществляется центральным органом. Сертификат выдается на срок до 5 лет.

Кроме указанных целей, сертификация средств защиты информации необходима также для решения вопросов экономической безопасности организации в связи с постоянным ростом компьютерных преступлений. Правовой основой предупреждения компьютерных преступлений является Указ Президента Российской Федерации "О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставление услуг в области шифрования информации" № 334 от 03.04.95 г. Приведем некоторые выдержки из данного указа:

– государственным организациям и предприятиям запрещено использование шифровальных средств, технических средств хранения, обработки и передачи информации, не имеющих сертификата;

– запрещено размещение государственных заказов на предприятиях, в организациях, использующих указанные средства, не имеющие сертификата;

– запретить деятельность физических и юридических лиц в области шифровальных и защищенных средств без лицензии;

– запретить ввоз на территорию России нелицензированных шифровальных средств и защищенной техники иностранного производства.

После получения сертификата на право оказания услуг за организацией осуществляется государственный контроль (надзор) по соблюдению требований технических регламентов.

Система аттестации объектов информатизации по требованиям безопасности информации является составной частью единой системы сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации и подлежит государственной регистрации в установленном порядке. Деятельность системы аттестации организует федеральный орган по сертификации продукции и аттестации объектов информатизации по требованиям безопасности информации федеральный орган по сертификации и аттестации, которым является ФСТЭК России.

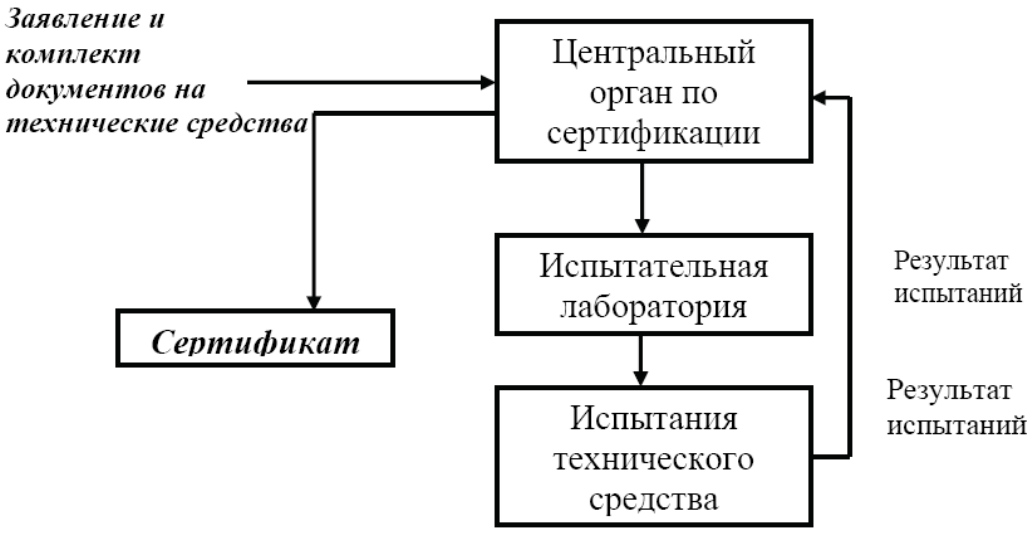


Рис. 1.4 Порядок сертификации технических средств

4. Аттестация объектов информатизации

Под **аттестацией объектов информатизации** понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа - "Аттестата соответствия" – подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных ФСТЭК России. Наличие на объекте информатизации действующего "Аттестата соответствия" дает право обработки информации с уровнем секретности (конфиденциальности) и на период времени, установленный в документе.

Обязательной аттестации подлежат объектыинформатизации, предназначенные для обработки информации,составляющей государственную тайну, и ведения секретныхпереговоров.

Аттестация предусматривает комплексную проверку защищаемого объекта информатизации в реальных условиях эксплуатации с целью оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности информации. Аттестация по требованиям безопасности информации предшествует началу обработки подлежащей защите информации и вызвана необходимостью официального подтверждения эффективности комплекса используемых на конкретном объекте информатизации мер и средств защиты информации. При аттестации объекта информатизации подтверждается его соответствие требованиям по защите информации от несанкционированного доступа, в том числе от компьютерных вирусов, от утечки за счет побочных электромагнитных излучений и наводок при специальных воздействиях на объект (высокочастотное навязывание и облучение, электромагнитное и радиационное воздействие), от утечки или воздействия на нее за счет специальных устройств, встроенных в объекты информатизации.

Аттестация объектов информатизации осуществляется в соответствии с Положением **«По аттестации объектов информатизации по требованиям безопасности информации», утвержденным председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.** устанавливает основные принципы, организационную структуру системы аттестации объектов информатизации по требованиям безопасности информации, порядок проведения аттестации, а также контроля и надзора за аттестацией и эксплуатацией аттестованных объектов информатизации.

Система аттестации объектов информатизации по требованиям безопасности информации (далее - система аттестации) является составной частью единой системы

сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации и подлежит государственной регистрации в установленном Госстандартом России порядке. Деятельность системы аттестации организует федеральный орган по сертификации продукции и аттестации объектов информатизации по требованиям безопасности информации (далее - федеральный орган по сертификации и аттестации), которым является ФСТЭК России.

Аттестация проводится органом по аттестации в установленном настоящим Положением порядке в соответствии со схемой, выбираемой этим органом на этапе подготовки к аттестации из следующего основного перечня работ:

– анализ исходных данных по аттестуемому объекту информатизации;

– предварительное ознакомление с аттестуемым объектом информатизации;

– проведение экспертного обследования объекта информатизации и анализ разработанной документации по защите информации на этом объекте с точки зрения ее соответствия требованиям нормативной и методической документации;

– проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств;

– проведение испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации;

– проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации;

– анализ результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждение заключения по результатам аттестации.

– Заявители:

– проводят подготовку объекта информатизации для аттестации путем реализации необходимых организационно-технических мероприятий по защите информации;

– привлекают органы по аттестации для организации и проведения аттестации объекта информатизации;

– предоставляют органам по аттестации необходимые документы и условия для проведения аттестации;

– привлекают, в необходимых случаях, для проведения испытаний несертифицированных средств защиты информации,

– используемых на аттестуемом объекте информатизации, испытательные центры (лаборатории) по сертификации;

– осуществляют эксплуатацию объекта информатизации в соответствии с условиями и требованиями, установленными в "Аттестате соответствия";

– извещают орган по аттестации, выдавший "Аттестат соответствия", о всех изменениях в информационных технологиях, составе и размещении средств и систем информатики, условиях их эксплуатации, которые могут повлиять на эффективность мер и средств защиты информации (перечень характеристик, определяющих безопасность информации, об изменениях которых требуется обязательно извещать орган по аттестации, приводится в "Аттестате соответствия");

– предоставляют необходимые документы и условия для осуществления контроля и надзора за эксплуатацией объекта информатизации, прошедшего обязательную аттестацию.

– Порядок проведения аттестации объектов информатизации по требованиям безопасности информации включает следующие действия:

– подачу и рассмотрение заявки на аттестацию;

– предварительное ознакомление с аттестуемым объектом;

– испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте (при необходимости);

– разработка программы и методики аттестационных испытаний;

– заключение договоров на аттестацию;

– проведение аттестационных испытаний объекта информатизации;

– оформление, регистрация и выдача "Аттестата соответствия";

– осуществление государственного контроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованных объектов информатизации;

– рассмотрение апелляций.

– На этапе аттестационных испытаний объекта информатизации:

– осуществляется анализ организационной структуры объекта информатизации, информационных потоков, состава и структуры комплекса технических средств и программного обеспечения, системы защиты информации на объекте, разработанной документации и ее соответствия требованиям нормативной документации по защите информации;

– определяется правильность категорирования объектов ЭВТ и классификации АС (при аттестации автоматизированных систем), выбора и применения сертифицированных и несертифицированных средств и систем защиты информации;

– проводятся испытания несертифицированных средств и систем защиты информации на аттестуемом объекте или анализ результатов их испытаний в испытательных центрах (лабораториях) по сертификации;

– проверяется уровень подготовки кадров и распределение ответственности персонала за обеспечение выполнения требований по безопасности информации;

– проводятся комплексные аттестационные испытания объекта информатизации в реальных условиях эксплуатации путем проверки фактического выполнения установленных требований на различных этапах технологического процесса обработки защищаемой информации;

– оформляются протоколы испытаний и заключение по результатам аттестации с конкретными рекомендациями по устранению допущенных нарушений, приведению системы защиты объекта информатизации в соответствие с установленными требованиями и совершенствованию этой системы, а также рекомендациями по контролю за функционированием объекта информатизации.

Заключение по результатам аттестации с краткой оценкой соответствия объекта информатизации требованиям по безопасности информации, выводом о возможности выдачи "Аттестата соответствия" и необходимыми рекомендациями подписывается членами аттестационной комиссии и доводится до сведения заявителя.

К заключению прилагаются протоколы испытаний, подтверждающие полученные при испытаниях результаты и обосновывающие приведенный в заключении вывод.

Протоколы испытаний подписываются экспертами – членами аттестационной комиссии, проводившими испытания.

Заключение и протоколы испытаний подлежат утверждению органом по аттестации.

1. 9 Лекция № 9 (2 часа).

Тема: «Разработка системы инженерно-технической защиты информации на критически важных объектах**»**

1.9.1 Вопросы лекции:

1. Разработка системы инженерно-технической защиты информации объекта
2. Рекомендации по выбору методов и средств инженерно-технической защиты

информации

3. Задачи и место инженерно-технической охраны в системе обеспечения информационной безопасности

1.9.2 Краткое содержание вопросов:

1. Разработка системы инженерно-технической защиты информации объекта

Способы и средства технической защиты информации применяются для создания вокруг объекта защиты преграды, препятствующей реализации угроз безопасности информации. В настоящее время проблема защиты информации относится к числу сложных, слабоформализуемых задач, решаемых на основе системного подхода.

Системный подход - это концепция решения сложных слабоформализуемых проблем, рассматривающая объект изучения (исследования) или проектирования в виде системы.

Основные принципы системного подхода состоят в следующем:

– любая система является подсистемой более сложной системы, которая влияет на структуру и функционирование рассматриваемой;

– любая система имеет иерархическую структуру, элементами и связями которой нельзя пренебрегать без достаточных оснований;

– при анализе системы необходим учет внешних и внутренних влияющих факторов, принятие решений на основе их небольшого числа без рассмотрения остальных может привести к нереальным результатам;

– накопление и объединение свойств элементов системы приводит к появлению качественно новых свойств, отсутствующих у ее элементов.

С позиции системного подхода совокупность взаимосвязанных элементов, функционирование которых направлено на обеспечение безопасности информации, образует ***систему защиты информации*.**

Такими элементами являются руководство и сотрудники службы безопасности, инженерные конструкции и технические средства, обеспечивающие защиту информации.

Система задается следующими характеристиками (рис. 9.1) – целями и задачами (конкретизированными в пространстве и во времени целями) :

– входами и выходами системы;

– ограничениями, которые необходимо учитывать при построении (модернизации, оптимизации) системы;

– процессами внутри системы, обеспечивающими преобразование входов в выходы.

Решение проблемы защиты информации с точки зрения системного подхода можно сформулировать как трансформацию существующей системы в требуемую.

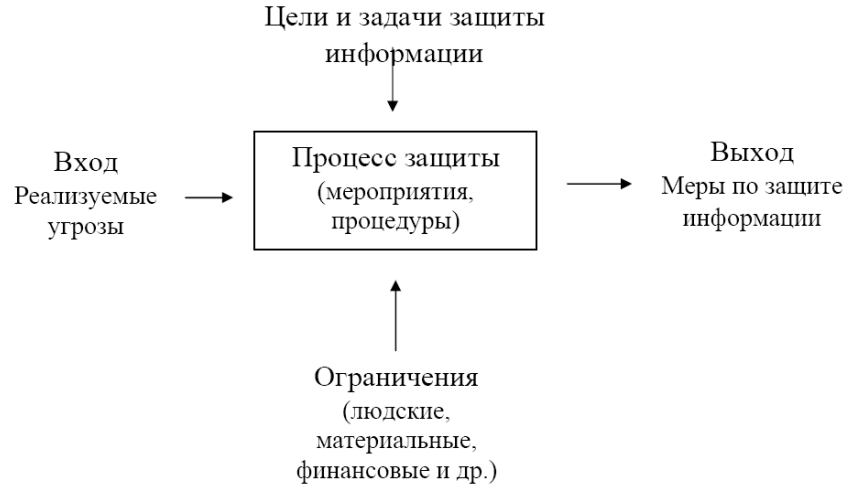


Рисунок 9.1. Основные характеристики системы защиты информации

Целью системы защиты является обеспечение требуемых уровней безопасности информации на объекте защиты. Задачи конкретизируют цели применительно к видам и категориям защищаемой информации, а также элементам объекта защиты и отвечают на вопрос, что надо сделать для достижения целей. Кроме того, уровень защиты нельзя рассматривать в качестве абсолютной меры, безотносительно от ущерба, который может возникнуть от потери информации и использования ее злоумышленником во вред владельцу информации. В качестве ориентира для оценки требуемого уровня защиты необходимо определить соотношение между ценой защищаемой информации и затратами на ее защиту. Уровень защиты рационален, когда обеспечивается требуемый уровень безопасности информации и минимизируются расходы на информацию. Эти расходы складываются из:

– затрат на защиту информации;

– ущерба за счет попадания информации к злоумышленнику и использования ее во вред владельцу.

Между этими слагаемыми существует достаточно сложная связь, так как ущерб из-за недостаточной безопасности информации уменьшается с увеличением расходов на ее защиту.

Если первое слагаемое может быть точно определено, то оценка ущерба в условиях скрытности разведки и неопределенности прогноза использования злоумышленником полученной информации представляет достаточно сложную задачу. Ориентировочная оценка ущерба возможна, если владелец информации ожидает получить от ее материализации определенную прибыль, которой он может лишиться в случае попадания ее конкуренту. Кроме того, последний, используя информацию, может нанести владельцу еще дополнительный ущерб, например за счет изменения тактики, продажи или покупки ценных бумаг и т. д. Дополнительные неблагоприятные факторы чрезвычайно трудно поддаются учету. Поэтому в качестве граничной меры для оценки ущерба можно использовать величину потенциальной прибыли, которую ожидает получить от информации ее владелец.

В свою очередь величина ущерба зависит от уровня защиты, определяемой расходами на нее. Максимальный ущерб возможен при нулевых расходах на защиту, минимальный – обеспечивается при идеальной защите. Однако идеальная защита требует бесконечно больших затрат.

Ограничения системы представляют собой выделяемые на защиту информации людские, материальные, финансовые ресурсы, а также ограничения в виде требований к системе. Суммарные ресурсы удобно выражать в денежном эквиваленте. Независимо от выделяемых на защиту информации ресурсов они не должны превышать суммарной цены защищаемой информации. Это верхний порог ресурсов.

Ограничения в виде требований к системе предусматривают принятие таких мер по защите информации, которые не снижают эффективность функционирования системы при их выполнении.

Входами системы инженерно-технической защиты информации являются:

– воздействия злоумышленников при физическом проникновении к источникам конфиденциальной информации с целью ее хищения, изменения или уничтожения;

– различные физические поля электрические сигналы, создаваемые техническими средствами злоумышленников и которые воздействуют на средства обработки и хранения информации;

– стихийные силы, прежде всего, пожара, приводящие к уничтожению или изменению информации;

– физические поля и электрические сигналы с информацией, передаваемой по функциональным каналам связи;

– побочные электромагнитные и акустические поля, а также электрические сигналы, возникающие в процессе деятельности объектов защиты и несущие конфиденциальную информацию.

Выходами системы инженерно-технической защиты информации являются меры по защите информации, соответствующие входным воздействиям.

Для защиты информации на основе системного подхода и анализа необходимо, наряду с организационным и техническим, методическое обеспечение, включающее комплекс методик и рекомендаций по проектированию систем инженерно-технической защиты информации на объектах защиты.

Задача проектирования или модернизации системы защиты информации и ее элементов возникает тогда, когда создается новая организация с информацией ограниченного доступа или существующая система не обеспечивает требуемый уровень безопасности информации.

Проектирование системы инженерно-технической защиты информации, обеспечивающей достижение поставленных целей и решение задач, проводится путем системного анализа существующей на объекте и разработки вариантов требуемой. Построение новой системы или ее модернизация предполагает:

– определение источников защищаемой информации и описание факторов, влияющих на ее безопасность;

– выявление и моделирование угроз безопасности информации;

– определение слабых мест существующей системы защиты информации;

– выбор рациональных мер предотвращения угроз;

– сравнение вариантов по частным показателям и глобальному критерию, выбор одного или нескольких рациональных вариантов;

– обоснование выбранных вариантов в докладной записке или в проекте для руководства организации;

– доработка вариантов или проекта с учетом замечаний руководства.

Типовой алгоритм проектирования инженерно-технической системы защиты информации представлен на рис. 9.2. Последовательность проектирования (модернизации) системы защиты включает три основных этапа:

– моделирование объектов защиты;

– моделирование угроз информации;

– выбор мер защиты.

Основным методом исследования систем защиты является моделирование, которое предусматривает создание модели и ее исследование (анализ). Описание или физический аналог любого объекта, в том числе системы защиты информации и ее элементов, создаваемые для определения и исследования свойств объекта, представляют собой его ***модель.*** В ней учитываются существенные для решаемой задачи элементы, связи и свойства изучаемого объекта.

Рисунок 9.2. Алгоритм проектированияинженерно-технической системы защиты информации

2. Рекомендации по выбору методов и средств инженерно-технической защиты информации

Так как не существует формальных методов синтеза вариантовпредотвращения угроз безопасности информации, то разработка мер по защите информации проводится эвристическим путем на основе знаний и опыта соответствующих специалистов. Однако в интересах минимизации ошибок процесс разработки должен соответствовать следующим рекомендациям .

Разработку мер защиты информации целесообразно начинать с угроз, имеющих максимальное значение, далее – с меньшей угрозой и так далее до тех пор, пока не будут исчерпаны выделенные ресурсы.

Такой подход гарантирует, что даже при малых ресурсах хватит средств для предотвращения наиболее значимых угроз. Для каждой угрозы разрабатываются меры (способы и средства) по защите информации.

Так как меры по защите информации рассматриваются для каждой угрозы, то в

контролируемой зоне возможно их дублирование. Так, полуоткрытая дверь в служебное помещение может способствовать как наблюдению за документами с экранов ПЭВМ в помещении, так и подслушиванию ведущихся в нем разговоров. Установленные на дверь устройство для автоматического ее закрытия и кодовый замок предотвращают утечку информации по этим каналам.

После объединения способов и средств защиты информации освобожденные ресурсы могут быть использованы для предотвращения очередных по рангу угроз.

Следовательно, разработка мер по предотвращению угрозпредставляет собой итерационный процесс, каждая итерация которого выполняется в 2 этапа:

- разработка локальных мер по предотвращению каждой из выявленных угроз;
- интеграция (объединение) локальных мер.

Условием для перехода к следующей итерации является освобождение в результате объединения способов и средств защиты информации части ресурса, достаточной для предотвращения очередной угрозы.

Совокупность рассмотренных планов и схем с результатами моделирования объектов защиты и угроз, а также предложений по способам и средствам защиты информации создают основу проекта по построению соответствующей системы или предложений по совершенствованию существующей системы.

В итоговой части проекта (служебной записке, предложениях) целесообразно оценить полноту выполнения задач по защите информации для выделенных ресурсов, а также нерешенные задачи и необходимые для их решения ресурсы.

Подготовленные документы (проект, служебная записка, предложения) предъявляются руководству для принятия решения.

Наличие в них нескольких вариантов решений способствует более активному участию в построении или совершенствованию системы защиты информации руководителя организации в качестве как наиболее опытного и квалифицированного специалиста, так и распорядителя ресурсов организации.

После принятия проекта (предложений) начинается этап их реализации. Основные задачи специалистов по защите информации заключаются в контроле за работами по выполнению организационных и технических мероприятий, участие в приемке результатов работ и проверке эффективности функционирования элементов и системы защиты в целом.

Результаты оформляются в виде предложений (проекта) в кратком сжатом виде, а материалы моделирования - в виде приложения с обоснованием предложений.

В заключение следует отметить, что материалы с предложениями и их обоснованием, в которых раскрываются методы и средства защиты информации, нуждаются в обеспечении высокого уровня безопасности, а обобщенные документы должны иметь наиболее высокий гриф из применяемых в организации.

3. Задачи и место инженерно-технической охраны в системе обеспечения информационной безопасности

Под несанкционированным доступом к информации (НСД) понимают доступ к информации (ознакомление, обработка, в частности, копирование, одификация или уничтожение информации), нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами информационной системы (ИС) - автоматизированными системами обработки данных (АСОД) или средствами традиционного документооборота .

При рассмотрении проблемы предотвращения НСД к информации пользуются понятиями субъекта и объекта доступа. Субъектами доступа к защищаемой информации могут быть:

– пользователи информации, когда они допущены к непосредственному участию в обработке и передаче информации, а также абоненты ИС, с которыми осуществляется обмен защищаемой информацией;

– обслуживающий персонал ИС в рамках выполнения своих функций.

В качестве нарушителя рассматривается субъект, осуществляющий несанкционированный доступ к информации. В случае защиты наиболее важных ИС необходимо учитывать, что нарушитель является специалистом высшей квалификации, знает все об ИС и, в частности, о системе и средствах ее защиты.

Объектами доступа являются, с одной стороны, технические средства ИС и помещения, в которых они расположены, а с другой стороны, непосредственно информационные ресурсы ИС.

Соответственно существуют следующие основные задачи защиты информации ИС от НСД :

– предотвращение доступа нарушителя в помещения, где размещены штатные средства ИС;

– предотвращение доступа нарушителя в информационную среду ИС и разграничение полномочий законных пользователей.

Первая задача решается в рамках инженерно-технических систем защиты информации объектов (рис. 2.1.), на которых размещены элементы ИС, путем предотвращения доступа нарушителя непосредственно к носителям информации в вычислительной среде.

Решение второй задачи связано с защитой информационных ресурсов непосредственно в информационной среде и основывается на введении правил доступа субъектов к объектам доступа. Контроль соблюдения правил доступа осуществляется системой разграничения доступа в рамках функционирования защищенной ИС.

Организационно – технические мероприятия по защите от НСД в ИС, обрабатывающих или хранящих информацию, отнесенную к государственной тайне, должны отвечать требованиям по обеспечению режима секретности проводимых работ, установленных в РФ, а все технические средства должны быть сертифицированы.

При обработке или хранении в ИС информации, не отнесенной к категории государственной тайны, для защиты конфиденциальной информации рекомендуется проведение следующих организационных – технических мероприятий :

– выявление конфиденциальной информации и ее документальное оформление в виде перечня сведений, подлежащих защите;

– определение и обеспечение порядка установления уровня полномочий субъекта доступа, а также круга лиц, которым это право предоставлено;

– установление и организацию правил разграничения доступа (ПРД), т.е. совокупности правил, регламентирующих права доступа субъектов к объектам;

– ознакомление субъекта доступа с перечнем защищаемых сведений и его уровнем полномочий, а также с организационно-распорядительной и рабочей документацией, определяющей требования и порядок обработки конфиденциальной информации;

– обеспечение охраны объекта, на котором расположена защищаемая ИС (территория, здания, помещения, хранилища носителей информации), путем установления соответствующих постов, технических средств охраны и т.п., предотвращающих или существенно затрудняющих хищение средств вычислительной техники (СВТ), носителей информации, а также НСД к СВТ и линиям связи;

– организация службы безопасности информации (ответственные лица, администратор ИС), осуществляющей учет, хранение и выдачу носителей информации, паролей, ключей, ведение служебной информации (генерацию паролей, ключей, сопровождение правил разграничения доступа), приемку включаемых в ИС новых программных средств, а также контроль за ходом технологического процесса обработки конфиденциальной информации и т.д.;

– разработка системы защиты информации от НСД, включая соответствующую организационно-распорядительную и эксплуатационную документацию;

– осуществление приемки системы защиты информации от НСД в составе ИС.

Структура комплекса технической защиты источников и носителей информации

Основу комплекса технической защиты источников и носителей информации составляют механические средства и инженерные сооружения, препятствующие физическому движению злоумышленника к месту нахождения объектов защиты, технические средства, информирующие сотрудников службы безопасности о проникновении злоумышленников в контролируемую зону и позволяющие наблюдать обстановку в них, а также средства и люди, устраняющие угрозы.

В соответствии с принципом многозональности и многорубежности защиты информации рубежи защиты создаются, прежде всего, на границах контролируемых (охраняемых) зон.

Состав системы инженерно-технической охраны объектов может существенно отличаться в зависимости от решаемых задач и финансовых возможностей: от деревянной двери с простым замком для большинства жилых квартир до автоматизированной интегральной системы охраны с группой быстрого реагирования.

В общем случае структура системы инженерно-технической охраны объектов представлена на рис 9.3.

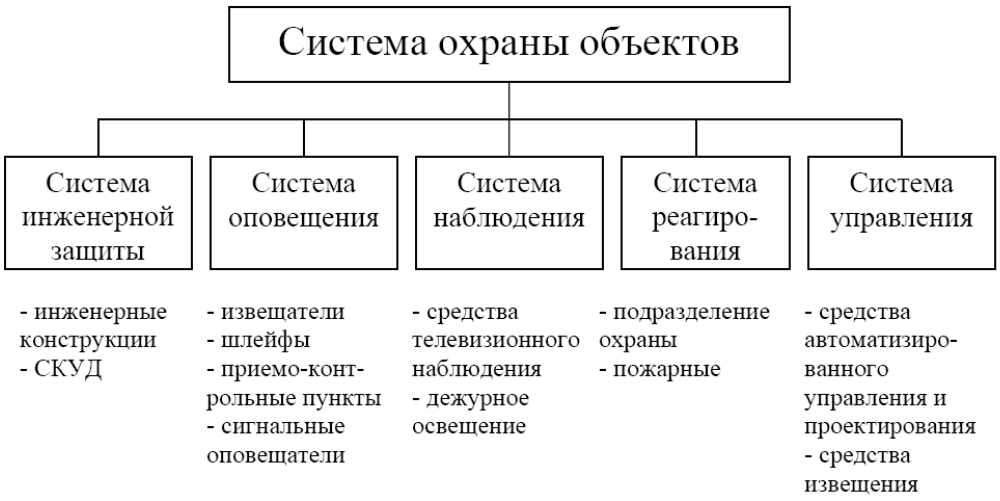


Рисунок 9.3 Структура системы охраны объектов

Система инженерной защиты предназначена для механического воспрепятствования проникновению злоумышленника к объектам защиты. Она включает инженерные конструкции, создающие механические преграды на пути злоумышленника, системы контроля и управления доступом людей и автотранспорта на охраняемую территорию.

Система оповещения должна оповещать сотрудников службы безопасности, прежде всего, охранников, органы вневедомственной охраны, милицию, пожарную охрану о проникновении злоумышленников на охраняемую территорию, о пожаре или иных стихийных бедствиях, защита от которых предусмотрена задачами системы. Основу этой подсистемы составляют технические средства охраны.

Все шире применяемые ***телевизионные средства наблюдения*** составляют основу ***системы наблюдения***. В нее входят также средства дежурного освещения, обеспечивающие необходимый уровень освещенности охраняемой территории в ночное

время. Подсистема наблюдения обеспечивает возможность визуального дистанционного контроля за охраняемой территорией и действиями злоумышленников.

Система реагирования имеет в своем составе людей и средства для физического и психологического воздействия на злоумышленников, проникших на охраняемую территорию, а также средства тушения пожара.

Персонал и средства ***системы управления*** обеспечивают работоспособность системы и управления ее элементами в различных ситуациях.

Эффективность системы технической охраны оценивают вероятностью обнаружения службой безопасности злоумышленника и пожара, а также временем перемещения злоумышленника на территории организации к источнику информации и обратно. Как видно на рис. 1.5 надежная защита обеспечивается совокупностью инженерных конструкций и технических средств, для приобретения и эксплуатации которых необходимы большие ресурсы, которые не имеют небольшие организации, а тем более физические лица. Проблема охраны в таких случаях решается объединением усилий нескольких организаций. В зависимости от структуры системы охраны разделяют на ***автономную и централизованную.***

В ***автономной системе*** все задачи по охране решаются в рамках одной организации, в централизованной – подсистемы нейтрализации угроз и управления являются общими для нескольких организаций.

Примером централизованной системы является охрана отделений филиалов сберегательного банка, мелких фирм, частных домов, дач, квартир. Некоторые рядом территориально расположенные фирмы, например в одном здании, могут иметь общее подразделение охраны.

Автономная система, в которой все структурные элементы расположены в пределах организации, имеет меньшее время на реакцию сил и средств для нейтрализации угроз на действия злоумышленника или пожар. В ней также проще поддерживать работоспособность технических средств.

В ***централизованной системе*** время на реакцию больше, особенно если охраняемая организация удалена на значительное расстояние от пункта централизованной охраны. Кроме того, это время может в ряде случаев недопустимо увеличено путем, например, случайного или созданного дорожно-транспортного происшествия с машиной охраны, следовавшей к объекту. Однако централизованные системы имеют большие возможности по нейтрализации угроз, особенно в виде вооруженного нападения.

В связи с этим можно сделать вывод, что крупные коммерческие структуры, располагающие необходимыми средствами, стремятся к созданию автономных систем охраны, а мелким организациям, а также гражданам выгоднее подключаться к централизованной системе охраны.

2. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ

2.1 Лабораторная работа № 1 (2 часа).

Тема: «Ознакомление со средствами добывания информации в оптическом диапазоне волн»

2.1.1 Цель работы:

Целью лабораторной работы является ознакомление студентов со средствами добывания информации в оптическом диапазоне волн.

2.1.2 Задачи работы:

1. Задачей лабораторной работы является классификация средств добывания информации в оптическом диапазоне волн.

2.1.3 Перечень приборов, материалов, используемых в лабораторной работе:

1. Персональный компьютер, специальное ПО

2.1.4 Описание (ход) работы:

В оптическом видимом диапазоне света информация разведкой добывается путем визуального, визуально-оптического и телевизионного наблюдения, фото- и киносъемки, а в инфракрасном диапазоне — с использованием приборов ночного видения и тепловизоров.

Наибольшее количество признаков добывается в видимом диапазоне. Но видимый свет как носитель информации имеет малую проникающую способность, дальность его распространения в атмосфере сильно зависит от ее состояния, климатических и погодных условий. ИК-лучи как носители информации обладают большей проникающей способностью и позволяют наблюдать объекты при малой освещенности и даже в темноте. Но при их преобразовании в видимый свет для обеспечения возможности наблюдения объекта человеком происходит значительная потеря информации об объекте.

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.

Большинство средств наблюдения представляют собой оптический приемник, содержащий оптическую систему, светоэлектрический элемент, усилитель и индикатор. В зависимости от вида светочувствительного элемента оптические приборы делятся 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).

Оптическая система или объектив проецирует световой поток от объекта наблюдения на поверхность светочувствительного элемента (сетчатку глаза, фотопленку, фотодиод, фототранзистор, мишень СЭП). Светочувствительный элемент преобразует оптическое изображение в эквивалентное распределение плотности химического вещества или электронное изображение, количество «свободных» электронов каждой точки которого пропорционально яркости соответствующей точки оптического изображения. Способы визуализации изображения для разных типов оптического приемника могут существенно отличаться. Изображение в виде зрительного образа формируется в мозгу человека, на фотопленке — в результате химической обработки светочувствительного слоя, на экране технического средства— путем параллельного или последовательного съема электронов со светоэлектрического элемента, усиления электрических сигналов и формирования под их действием видимого изображения на экране оптического приемника.

Характеристики средств наблюдения определяются, прежде всего, параметрами оптической системы и светоэлектрического элемента, а также зависят от способов обработки электрических сигналов и формирования изображения при индикации. Основными характеристиками являются:

•диапазон длин волн световых лучей, воспринимаемых средством наблюдения;

•чувствительность;

•разрешающая способность;

•поле (угол) зрения и изображения;

•динамический диапазон интенсивности света на входе оптического приемника, не вызывающий искажение изображения на его выходе.

Средства наблюдения в зависимости от назначения создаются для видимого диапазона длин волн или его отдельных участков (зон), а также для различных участков инфракрасного диапазона.

Чувствительностьсредства наблюдения оценивается минимальным уровнем световой энергии, при которой обеспечивается требуемое качество изображения объекта наблюдения. Качество изображения зависит как от яркости и контрастности проецируемого изображения, так и от помех. Помехи создают лучи света, попадающие на вход приемника от других источников света, и тепловые Шумы светоэлектрического преобразователя. На экране светочувствительного элемента при посторонней внешней засветке ухудшается контраст изображения аналогично варианту прямого попадания на экран телевизионного приемника или монитора компьютера яркого солнечного света.

Разрешающая способностьхарактеризуется минимальными линейными или угловыми размерами между двумя соседними точками изображения, которые наблюдаются как отдельные. Так как изображение формируется из точек (пикселей), размеры которых определяются разрешающей способностью средства наблюдения, то вероятность обнаружения и распознавания объекта возрастает с повышением разрешающей способности средства наблюдения (увеличением количества пикселей изображения объекта).

Размеры наблюдаемой части пространства характеризуются **полем и углом зрения.**Поле зрения — часть пространства, изображение которого проецируется на экран оптического приемника. Угол, под которым средство «видит» предметное пространство, называется **углом поля зрения.**Часть поля зрения, удовлетворяющего требованиям к качеству изображения по резкости, называется **полем**или, соответственно, **углом поля изображения.**

Динамический диапазоноптического приемника определяет в дБ интервал силы света на входе оптического приемника, при котором обеспечивается заданное качество изображения на выходе. Чем шире динамический диапазон оптического приемника, тем больше оперативные возможности его применения. Несоответствие динамического диапазона приемника диапазону силы света от объектов наблюдения приводит не только к искажению добываемой информации, но и может вызвать нарушение в работе приемника вплоть до разрушения светочувствительного элемента. Например, если человек посмотрит открытыми глазами на Солнце, то он в течение некоторого времени «слепнет».

Наиболее совершенным средством наблюдения в видимом диапазоне является зрительная система человека, включающая глаза и области мозга, осуществляющие обработку сигналов, поступающих с сетчатки глаз. Возможности зрения человека характеризуются следующими показателями:

•глаз воспринимает световые лучи в диапазоне 0,4-0,76 мкм, причем максимум его спектральной чувствительности в светлое время суток приходится на голубой цвет (0,51 мкм), в темноте — на зеленый (0,55 мкм);

•порог угловых размеров, которые глаз различает как две раздельные точки на объекте наблюдения, составляет днем 0,5-1 угл. мин, ночью — 30 угл. мин;

• порог контрастности различимого объекта по отношению к фону составляет днем 0,01-0,03, ночью — 0,6;

• диапазон освещенности объектов наблюдения, к которым адаптируется глаз, достигает 60-70 дБ;

•при освещенности менее 0,1 лк (в безоблачную лунную ночь) глаз перестает различать цвет;

•угловое поле зрения:

—в горизонтальной плоскости 65-95°;

—в вертикальной плоскости 60-90°;

— резкого изображения 30°;

•расстояние наилучшего зрения — 250 мм;

•время удержания взглядом изображения — 0,06 С;

Уникальные возможности зрительной системы человека обеспечиваются, прежде всего, оптической системой глаза, выполняющего функции объектива. Ее возможности и достигаются в результате того, что его кривизна с помощью специальных глазных мышц изменяется таким образом, чтобы обеспечить на сетчатке глаза максимально четкое изображение объектов, расположенных на различных расстояниях от наблюдателя. Хотя ведутся исследования по созданию подобных искусственных объективов, но приблизиться к возможностям глаза пока не удается.

Оптические системы

Основу оптических систем средств наблюдения составляют объективы, которые в силу постоянства сферической кривизны поверхностей линз и оптической плотности стекла проецируют изображения с различного рода погрешностями. Наиболее заметны следующие из них:

•сферическая аберрация, проявляющаяся в отсутствии резкости изображения на всем поле зрения (оно резко в центре или по краям);

•астигматизм— отсутствие одновременной резкости на краях поля изображения для вертикальных и горизонтальных линий;

•дисторсия — искривление прямых линий на изображении;

•хроматическая аберрация — появление цветных окантовок на границах световых переходов изображения, вызванных различными коэффициентами преломления линзами объектива спектральных составляющих световых лучей.

С целью уменьшения погрешностей объективы выполняются из большого (до 10 и более) количества сферических линз с различной кривизной поверхностей. Все или отдельные группы линз склеиваются между собой. Аберрации линз существенно уменьшаются у асферических линз со сложной кривизной поверхности. Технология полировки асферических линз сложна и дорога. Выпускаются для недорогих объективов литые асферические линзы, уступающие по качеству стекла шлифованным сферическим линзам.

Возможности объективов описываются совокупностью характеристик, основными из которых являются:

•фокусное расстояние;

•угол поля зрения и изображения;

•светосила;

•разрешающая способность;

•частотно-контрастная характеристика.

Фокусное расстояниеобъектива представляет собой расстояние от оптической плоскости объектива до плоскости, где фокусируются входящие в объектив параллельные лучи света. По соотношению величины фокусного расстояния f объектива и длины диагонали кадра поля создаваемого им изображения d объективы делятся на короткофокусные, у которых $f < d$, нормальные или среднефокусные ($f \sim d$), длиннофокусные и телеобъективы с $f > d$, а также с переменным фокусным расстоянием. Фокусное расстояние глаза человека составляет около 17 мм. Значения фокусного расстояния объективов унифицированы и принимают дискретные значения: 2,6, 3,5,4,8, 6, 8, 12, 16, 25, 50, 75 мм и т. д.

Объектив с переменным фокусным расстоянием (панкреатический) представляет собой сложную оптическую систему, в которой предусмотрена возможность смещения оптических компонентов вдоль оптической оси объектива, за счет чего изменяется величина фокусного расстояния. Величину фокусного расстояния изменяют **дискретно или плавно.**Дискретное изменение фокусного расстояния достигается применением **афокальных насадок,**уменьшающих или увеличивающих фокусное расстояние. Плавное изменение величины фокусного расстояния осуществляется перемещением отдельных линз объектива вдоль оптической оси по линейному или нелинейному закону. В зависимости от способа изменения эти объективы подразделяют

на **вариообъективы и трансфокаторы.**Вариообъективы представляют собой единую оптическую схему, в которой изменение фокусного расстояния осуществляется непрерывным перемещением одной или нескольких линз вдоль оптической оси. Трансфокаторы состоят из насадки с переменным плавным увеличением и объектива с постоянным фокусным расстоянием.

Сложность оптической конструкции объективов с переменным фокусным расстоянием вызвана, прежде всего, тем, что при изменении фокусного расстояния должно автоматически сохраняться положение плоскости резкого изображения наблюдаемого объекта. Добиваются этого путем оптической или механической компенсации. В первом случае кратность изменения фокусного расстояния не более 3, во втором — 6-7.

По **углу поля зрения (изображения)**различают узкоугольные объективы, у которых величина этого угла не превышает 30°, среднеугольные (угол в пределах 30°-60°), широкоугольные с углом более 60° и, наконец, — с переменным углом поля изображения у объективов с переменным фокусным расстоянием.

Чем больше фокусное расстояние f объектива, тем больше масштаб изображения и больше деталей объекта можно рассмотреть на изображении, но тем меньше угол поля зрения. Поэтому для обнаружения объекта используют короткофокусные объективы, а Для распознавания — длиннофокусные.

Светосилахарактеризует долю световой энергии, пропускаемой объективом к светочувствительному элементу. Очевидно, что чем выше светосила объектива, тем ярче изображение на светочувствительном элементе. На светосилу объектива влияют следующие факторы:

•относительное отверстие объектива;

•прозрачность (коэффициенты пропускания, поглощения, отражения) линз;

•масштаб изображения;

•коэффициент снижения яркости изображения к краю его поля.

Светосила без учета реальных потерь света в линзах вычисляется как квадрат относительного отверстия, равного d/f, где d — диаметр входного отверстия (апертуры). Эффективное относительное отверстие объектива меньше геометрического на величину потерь света в его линзах. По величине относительного отверстия объективы делятся на **сверхсветосильные с d/f > 1/2, светосильные**с d/f = 1/2,8-1/4) и **малосветосильные**с d/f < 1/5 [5]. В зарубежной литературе в качестве характеристики светосилы объектива используют такой показатель, как «фокальное число» F = f/d. У человека с f=17 мм и d = 6мм F = 2,8, т. е. хрусталик глаза относится к светосильным объективам. Чем больше светосила объектива, тем выше чувствительность средства наблюдения. Однако при этом растут искажения изображения и для их уменьшения усложняют конструкцию светосильных объективов, что естественно приводит к их удорожанию. Для изменения относительного отверстия при чрезмерно большом диапазоне освещенности объекта наблюдения и повышения глубины резкости в объективе устанавливается механизм регулировки диаметра относительного отверстия — диафрагма. Величина диафрагмы изменяется вручную или автоматически.

Свет, падающий на линзу и проходящий через нее, отражается и поглощается. Количество поглощенного света зависит от толщины стекла (в среднем 1-2% на 1 см толщины). Линзы отражают 4-6% падающего на них света. Чем больше отражающих поверхностей имеет объектив, тем больше потери света. В объективах из 5-7 линз потери света на отражение могут составлять 40-50% [5]. Кроме того, свет, отраженный от внутренних поверхностей линз в сторону плоскости изображения, накладывается на изображение и создает помеху в виде засветки изображения. Засветка уменьшает контраст изображения. Эти неблагоприятные факторы, возникающие в многолинзовых объективах, уменьшают просветлением линз.

Просветлениемназывается способ уменьшения переотражения света от внутренних поверхностей линз путем нанесения на них тонкой пленки. Толщина просветляющей пленки должна составлять 1/4 длины волны падающего на линзу света. Пленка сдвигает фазу отраженной от внутренней поверхности линзы волны на 180°, вследствие чего она компенсируется падающей волной. Первоначально объективы просветляли для узких участков спектра. Просветленный объектив в отраженном свете приобретал сине-фиолетовый оттенок и назывался «голубой» оптикой. Современные технологии просветления оптики позволяют наносить на поверхность линзы 12-14 слоев просветляющих пленок и перекрывать тем самым весь спектр видимого диапазона света. Такую оптику маркируют индексами МС — многослойное покрытие. Объективы МС в отраженном свете не меняют цвет.

Возможность объектива передавать мелкие детали изображения оценивается **разрешающей способностью.**Она выражается максимальным числом N штрихов и промежутков между ними на 1 мм поля изображения в его центре и по краям. Наиболее высокую разрешающую способность имеют объективы для микрофотографирования в микроэлектронике и линзы астрономических телескопов. Она достигает 1000 и более линий на мм. Изготовление таких объективов является чрезвычайно трудоемким процессом продолжительностью для линз телескопов большого диаметра в течение многих месяцев. Объективы с линзами из кварца, применяемые в фотографии, имеют существенно меньшее разрешение порядка 50 лин./мм, с штампованными из синтетических материалов линзами — еще ниже.

Так как одним из основных факторов, определяющих вероятность обнаружения и распознавания объектов, является контраст его изображения по отношению к фону, то важной характеристикой объектива как элемента средства наблюдения является **его частотно-контрастная характеристика.**Она служит мерой способности объектива передавать контраст деталей объекта и измеряется отношением контрастности деталей определенных размеров на изображении и на объекте. Уменьшение контраста мелких деталей на изображении вызвано тем, что в результате различных аберраций объектива на изображении размываются границы деталей наблюдаемых объектов.

Для количественной оценки частотно-контрастной характеристики в качестве исходного объекта используется эталонный объект наблюдения — мира в виде черно-белых линий с уменьшающейся шириной, нанесенных, например, тушью на белой бумаге. По результатам измерений контрастности п линий на проецируемом объективом изображении строится зависимость контраста К от количества линий п в одном мм. Зависимость К = f(n) определяет частотно-контрастную характеристику объектива.

В связи с большими техническими проблемами создания универсальных объективов с высокими значениями показателей, оптическая промышленность выпускает широкий набор специализированных объективов: для фото- и киносъемки, портретные, проекционные, для микрофотографирования и т. д.

Для добывания информации применяются объективы трех видов: для аэрофотосъемки, широкого применения (фото-, кино- и видеосъемки с использованием бытовых и профессиональных камер) и для скрытой съемки.

Объективы широкого применения разделяются в соответствии с размерами фотоаппаратов: для малоформатных и миниатюрных, среднеформатных и крупноформатных камер.

Для скрытого наблюдения используются:

•телеобъективы с большим фокусным расстоянием (300-4800 мм)для фотографирования на большом удалении от объекта наблюдения, например из окна противоположного дома и далее;

•так называемые точечные объективы для фотографирования из портфеля, часов, зажигалки, через щели и отверстия. Они имеют очень малые габариты и фокусное расстояние, но большой угол поля зрения.

Например, объектив фотоаппарата РК 420, вмонтированного в корпус наручных часов, имеет размеры 7,5 мм с апертурой 2,8 мм. В миникамерах фирм Hitachi, Sony, Philips, Ockar используются объективы диаметром 1-4 мм и длиной до 15 мм.

2.2 Лабораторная работа № 2 (2 часа).

Тема: «Ознакомление со средствами добывания информации в акустическом диапазоне волн**»**

2.2.1 Цель работы:

Целью лабораторной работы является закрепление у студентов знаний о технических каналах утечки речевой конфиденциальной информации и выработка практических навыков работы с контрольно-измерительной аппаратурой, регистрирующей акустические и виброакустические колебания в различных средах их распространения.

2.2.2 Задачи работы:

1. Задачей лабораторной работы является проведение инструментально-расчетной оценки защищенности помещения от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам.

2.2.3 Перечень приборов, материалов, используемых в лабораторной работе:

1. Персональный компьютер, специальное ПО

2.2.4 Описание (ход) работы:

1.Состав средств измерений и вспомогательного оборудования

Для проведения измерений уровней акустических (вибрационных) сигналов в помещении и контрольных точках используются типовые средства измерений и вспомогательное оборудование, из которых собираются формирователь акустического тест-сигнала и измерители акустических (вибрационных) сигналов и шумов.

В состав формирователя акустического тест-сигнала входят:

- генератор сигналов (ГС) иди генератор шума (ГШ);
- усилитель мощности (УМ);
- акустический излучатель (АИ)- громкоговоритель или звуковая колонка.

В состав измерителя акустического сигнала и акустического шума входят:

- измерительный микрофон;
- микрофонный усилитель;
- измеритель шума и вибраций (шумомер).

В состав измерителя вибрационного сигнала и вибрационного шума входят:

- измерительный вибродатчик (акселерометр);
- предусилитель вибродатчика;
- измеритель шума и вибраций (шумомер). Требуемые технические характеристики средств измерений и вспомогательного оборудования приведены в приложении 1.

2. Порядок размещения средств измерений и вспомогательного оборудования при проведении измерений

2.1. Размещение акустического излучателя в помещении:

- если ограждающей конструкцией (ОК) является стена, дверь или окно, то АИ необходимо размещать на высоте 1-1,5 м от пола и на расстоянии 1,5 м от ОК. Ось апертуры АИ направляется в сторону ОК по нормали к ее поверхности;
- если ОК является пол, то АИ необходимо размещать в центре помещения на высоте 1-1,5 м от пола. Ось апертуры АИ направляется в сторону пола по нормали к его поверхности;
- если ОК является потолок, то АИ необходимо размещать в центре помещения на высоте 1-1,5 м от пола. Ось апертуры АИ направляется в сторону потолка по нормали к

его поверхности.

Размещение АИ относительно элементов ИТС производится аналогично.

2.2. Размещение микрофона при измерении уровня излучаемого тест-сигнала в помещении:

- измерительный микрофон размешается на осевой линии апертуры АИ на расстоянии 1 м от плоскости апертуры и на расстоянии 0,5 м от поверхности ОК или элемента инженерно-технических сооружений (ИТС).

2.3. Размещение микрофона при измерении уровня акустического сигнала и акустического шума в КТ:

- измерительный микрофон размещается в выбранной точке контроля на расстоянии 0,5 м от поверхности ОК.

2.4. Размещение вибродатчика (акселерометра) при измерении уровня вибрационного сигнала и вибрационного шума в КТ:

- измерительный вибродатчик размешается в выбранной КТ непосредственно на поверхности ОК или на поверхности контролируемого элемента ИТС.

3. Условии проведения измерений

Измерения необходимо проводить при минимальных уровнях акустических и вибрационных шумов в помещении и КТ (при отсутствии персонала в помещении, выключенных системах вентиляции, кондиционирования и других источников дискретных шумов, при отсутствии транспортных шумов и пр.).

2.3 Лабораторная работа № 3 (2 часа).

Тема: «Ознакомление со средствами добывания информации в радиоэлектронном канале утечки**»**

2.3.1 Цель работы:

Целью лабораторной работы является ознакомление студентов со средствами добывания информации в радиоэлектронном канале утечки

2.3.2 Задачи работы:

1. Задачей лабораторной работы является проведение инструментально-расчетной оценки защищенности помещений от утечки конфиденциальной информации в радиоэлектронном канале **.**

2.3.3 Перечень приборов, материалов, используемых в лабораторной работе:

1. Персональный компьютер, специальное ПО

2.3.4 Описание (ход) работы:

1 Классификация акустоэлектрических преобразователей но физическим процессам, создающим опасные сигналы, приведена на рис. 1.

На выходе активных акустоэлектрических преобразователей под действием акустической волны возникают электрические сигналы. У пассивных акустоэлектрических преобразователей те же действия акустической волны вызывают лишь изменения параметров преобразователей.

По способам формирования электрического сигнала активные акустоэлектрические преобразователи могут быть электродинамическими, электромагнитными и пьезоэлектрическими.

Опасные сигналы в электродинамических акустоэлектрических преобразователях возникают в соответствии с законом электромагнитной индукции при перемещении провода в магнитном поле под воздействием акустической волны. Если провод длиной L под действием акустической волны со звуковым давлением P перемешается со скоростью V в магнитном поле с индукцией B, то в нем при условии перпендикулярности силовых магнитных линий проводу и скорости его перемещения, возникает ЭДС величиной E = LBV. Так как $V=PS/Z_{мс}$ (P - звуковое давление, S - площадь провода, на которую

оказывает давление акустическая волна, $Z_{мс}$ - величина механического сопротивления движению провода), то $E = LBSP/ Z_{мс}$.

Рис. 1. Классификации акустоэлектрических преобразователей

Наибольшей чувствительностью обладают электродинамические акустоэлектрические преобразователи в виде динамических головок громкоговорителей.

Сущность преобразования состоит в следующем. Под давлением акустической волны соединенная с диффузором катушка в виде картонного цилиндра с намотанной на нем тонкой проволокой перемещается в магнитном поле, создаваемым постоянным магнитом цилиндрической формы. В соответствии с законом электромагнитной индукции в проводах катушки возникает ЭДС, величина которой пропорциональна громкости звука.

Аналогичный эффект возникает в *электромагнитных акустоэлектрических преобразователях.* К ним относятся электромагниты электромеханических звонков и капсюлей телефонных аппаратов, шаговые двигатели вторичных часов, кнопочные извещатели ручного вызова пожарной службы охраняемого объекта и др. Электрические сигналы индуцируются в катушках электромагнитов этих устройств в результате изменений напряженности создаваемых ими полей, вызванных изменениями под действием акустической волны воздушного зазора между сердечником и якорем электромагнита или статора (неподвижной части) и ротора (подвижной части) электродвигателя.

Перечень бытовых радио- и электроприборов, в которых возникают подобные процессы и которые устанавливаются в служебных и жилых помещениях, достаточно велик. К ним относятся телефонные аппараты с электромеханическими звонками, вторичные часы системы единого времени предприятия или организации, вентиляторы и др. Уровни опасных сигналов в этих цепях зависят от конструкции конкретного типа средства и их значения имеют значительный разброс. Например, опасные сигналы в звонковой цепи телефонного аппарата могут достигать единиц мВ.

Активными акустоэлектрическими преобразователями являются также некоторые кристаллические вещества (кварц, сегнетовая соль, титанат и ниобат бария и др.), которые широко применяются в радиоаппаратуре для стабилизации частоты и фильтрации сигналов, в качестве акустических излучателей сигналов вызова в современных телефонных аппаратах вместо электромеханических звонков. На поверхности этих веществ при механической деформации их кристаллической решетки (давлении на поверхность, изгибе, кручении) возникают электрические заряды.

В пассивных акустоэлектрических преобразователях акустическая волна изменяет

параметры элементов схем средств, в результате чего изменяются параметры циркулирующих в этих схемах электрических сигналов. В большинстве случаев под действием акустической волны изменяются параметры индуктивностей и емкостей электрических цепей. В соответствии с этим акустоэлектрические преобразователи называются *индуктивными и емкостными.*

Если схема электрической цепи содержит катушку с витками проволок, то под воздействием акустической волны изменяются расстояние между витками и геометрические размеры самой катушки. В результате этого, как следует из соответствующих формул, изменяется индуктивность катушки. Если, например, катушка является элементом частотно-задающего контура генератора, то изменение индуктивности вызывает частотную модуляцию сигнала генератора. В итоге информация, записанная в параметры акустической волны, переписывается в параметры электрического сигнала, способного перенести ее к злоумышленнику на большое расстояние. Аналогичная картина наблюдается при изменении под действием акустической волны емкости контура генератора.

Если акустоэлектрический преобразователь представляет собой реактивное сопротивление, величина которого меняется в соответствии с параметрами акустического сигнала, то изменение этого сопротивления вызывает амплитудную модуляцию тока в цепи.

Разновидностью индуктивного является магнитострикционный акустоэлектрический преобразователь. *Магнитострикция* проявляется в изменении магнитных свойств ферромагнитных веществ (электротехнической стали и ее сплавов) при их деформировании (растяжении, сжатии, изгибании, кручении). Этот эффект обусловлен изменением под действием механических напряжений доменной структуры ферромагнетика и называется *обратной магнитострикцией.* Прямая магнитострикция заключается в изменении геометрических размеров и объема ферромагнитного тела при помещении его в магнитное поле. В результате обратной магнитострикции под действием акустической волны изменяется магнитная проницаемость сердечников контуров, дросселей, трансформаторов радио- и электротехнических устройств. Что приводит к эквивалентному изменению значений индуктивностей цепи и модуляции протекающих через них высокочастотных сигналов.

Итак, к наиболее распространенным случайным акустоэлектрическим преобразователям относятся:

- вызывные устройства телефонных аппаратов;
- динамические головки громкоговорителей, электромагнитные капсюли телефонных трубок, электрические двигатели вторичных часов системы единого времени и бытовых электроприборов;
- катушки контуров, дросселей, трансформаторов, провода монтажных жгутов, пластины (электроды) конденсаторов;
- пьезоэлектрические вещества (кварцы генераторов, виброакустические излучатели акустических генераторов помех);
- ферромагнитные материалы в виде сердечников трансформаторов и дросселей.

Угроза информации от акустоэлектрического преобразования зависит, прежде всего, от его *чувствительности,* которая характеризуется отношением величины электрического сигнала на его выходе или изменения падающего на нем напряжения к силе звукового давления на поверхность чувствительного элемента преобразователя на частоте F = 1000 Гц и измеряется в В/Па или мВ/Па. Очевидно, чем выше чувствительность преобразователя, тем больше потенциальная угроза от него для безопасности акустической информации.

Чувствительность в мВ/Па некоторых акустоэлектрических преобразователей приведена в таблице 1.

Таблица 1

№ п/п	Акустоэлектрический преобразователь	Чувствительность, мВ/Па
1	Электродинамический микрофон	4-6
2	Электродинамический громкоговоритель	2-3
3	Абонентский громкоговоритель	30-45
4	Вторичные электрические часы	0,1-0,5
5	Электромеханический звонок телефонного аппарата	0,05-0,06
6	Пьезоэлектрическое вызывное устройство телефонного аппарата	8-11
7	Телефонный капсюль	3-5
8	Электромагнитное реле	0,04-0,5
9	Трансформаторы, дроссели	0,001-0,2

Опасные сигналы, образованные акустоэлектрическими преобразователями, могут распространяться по проводам, выходящим за пределы контролируемой зоны, излучаться в эфир, модулировать другие, более мощные электрические сигналы, к которым возможен доступ злоумышленников. При этом надо иметь в виду, что чувствительность современных радиоприемников и усилителей электрических сигналов превышает в десятки и сотни раз уровни наиболее распространенных опасных сигналов. Следовательно, опасными сигналами на выходе акустоэлектрических преобразователей, имеющими даже весьма малые значения (доли милливольт), нельзя пренебрегать и необходимо уметь оценивать степень их опасности.

2. Метод оценки заключается в инструментально-расчетном определении совокупности октавных отношений напряжений (отношении «сигнал/шум» по напряжению Δi), наводимых в функциональных (сигнальных) цепях ВТСС тестовым акустическим сигналом и шумом за счет их акустоэлектрических преобразований соответствующими системами и средствами и последующим сравнением этих отношений с нормативными значениями.

3. Определение отношений «сигнал/шум» проводится на разъемах функциональных (сигнальных) цепей ВТСС при отключенных линиях, выходящих за пределы помещения, в октавных полосах частот со среднегеометрическими частотами f_{cpi}, равными 250. 500, 1000, 2000,4000 Гц,

4. Инструментальным способом определяется величина напряжения шума $U_{ш,npi}$ и величина напряжения смеси тест-сигнала и шума $U_{(с+ш)i}$ по усреднению результатов пяти отдельных измерений.

5. Расчетным способом находятся приведенные к ширине октавной полосы частот напряжения: шума $U_{ш.октi}$, тест-сигнала U_{ci} и отношения напряжении тест-сигнала и шума $\Delta i = U_{ci} / U_{ш.октi}$

6. В качестве тест-сигнала используются перестраиваемые по частоте в октавных полосах гармонические (тональные) частоты. Октавные уровни излучаемого тест-сигнала должны соответствовать интегральному уровню речи 70 дБ (для помещений не оборудованных системами звукоусиления) и 84 дБ (для остальных помещений). Значения октавных уровней тест-сигнала приведены в таблице 2.

Таблица 2

Среднегеометрические частоты октавных полос, Гц	Ширина октавной полосы, Гц	Октавные уровни тест-сигналов, дБ (Па), для речи с интегральным уровнем 70 дБ	Октавные уровни тест-сигналов, дБ (Па), для речи с интегральным уровнем 84 дБ
250	175	66 (0,04)	80 (0,2)

500	350	66 (0,04)	80 (0,2)
1000	700	61 (0,02)	75 (0,1)
2000	1400	56 (0,01)	70 (0,06)
4000	2800	53 (0,009)	67 (0,04)

Перевод уровней речевого сигнала из размерности *L (дБ)* в размерность *L (Па)* произведшей по формуле

$$L(Па) = 2 \cdot 10^{-5} \cdot 10^{0,05L(дБ)}$$

Уровень излучаемого тест-сигнала должен быть стабилен в процессе проведения измерений. Все измерения должны проводиться в соответствии с инструкцией по эксплуатации применяемых средств измерений

Для обеспечения защищенности помещения от утечки речевой конфиденциальной информации по акустоэлектрическим каналам нормативное значение Δi на разъемах функциональных (сигнальных) цепей каждого потенциально опасного ВТСС в каждой октавной полосе (175...350 Гц, 350...700 Гц, 700...1400 Гц, 1400 ...2800 Гц и 2800...5600 Гц) должно отвечать условию $\Delta i \leq 0,3$.

2.4 Лабораторная работа № 4 (2 часа).

Тема: «Ознакомление со средствами добывания информации в электромагнитном канале утечки**»**

2.4.1 Цель работы:

Целью лабораторной работы является освоение студентами методики оценки защищенности основных технических средств и систем (ОТСС), предназначенных для обработки, хранения и передачи по линиям связи конфиденциальной информации, от утечки информации за счет побочных электромагнитных излучений (ПЭМИ).

2.4.2 Задачи работы:

1. Задачей лабораторной работы является проведение инстру-ментально-расчетной оценки требуемого радиуса контролируемой зоны для различных ОТСС.

2.4.3 Перечень приборов, материалов, используемых в лабораторной работе:

1. Персональный компьютер, специальное ПО

2.4.4 Описание (ход) работы:

Теоретическое введение

Одним из основных и опасных каналов несанкционированного доступа к конфиденциальной информации является перехват ПЭМИ от работающих ОТСС. Методами перехвата являются поиск сигналов, выделение из них информативных с дальнейшей обработкой и анализом.

Этот канал по сравнению с другими каналами имеет ряд преимуществ: оперативность и достоверность получаемой информации, возможность без риска съема в любое время, скрытность получении, возможность обнародования без угрозы перекрытия канала. Поэтому одной из важнейших задач при осуществлении мероприятий по защите информации является определение требуемого радиуса контролируемой зоны объекта информатизации.

Побочные электромагнитные излучения (ПЭМИ) составляют физическую основу для утечки конфиденциальной информации при ее обработке (передаче) основными техническими средствами и системами

Характер распространения электромагнитного поля в свободном пространстве описывается четырьмя уравнениями Максвелла, приведенными им в 1873 г. в труде «Трактат об электричестве и магнетизме». Эти уравнения явились обобщением ранее

открытых законов электрического и магнитного полей.

В соответствии с первым уравнением любое магнитное по¬ле создается электрическими токами и изменением во времени электрического поля. Второе уравнение обобщает закон электромагнитной индукции. Открыт Фарадеем в 1831 г. и указывает на то, что в результате изменения магнитного поля в любой сре¬де появляется электрическое поле. Из третьего уравнения Мак¬свелла следует, что поток вектора электрической индукции через любую замкнутую поверхность равен сумме зарядов в объеме, ограниченном этой поверхностью. Четвертое уравнение позво¬ляет сделать вывод о том, что число силовых линий магнитного поля, входящих в среду некоторого объема, равно числу сило¬вых линий, выходящих из этого объема. Это возможно при ус¬ловии отсутствия в природе магнитных зарядов.

Из уравнений Максвелла следует также, что автономно (не¬зависимо) в природе могут существовать только постоянные электрические и магнитные поля. Поле, излучаемое зарядами и токами переменной частоты, является электромагнитным. В нем присутствуют электромагнитные и электрические компоненты, которые описываются взаимно перпендикулярными векторами. В зависимости от вида излучателя и расстояния от него до точки измерения характер изменения и соотношения между этими компонентами отличаются и изменяются. Характер распространения электромагнитного поля поддается точному математиче¬скому описанию для моделей излучателей в виде элементарных вибраторов. В качестве элементарного вибратора рассматривает¬ся модель излучателя, размеры которой существенно меньше длины волны излучаемого электромагнитного поля и расстояния от излучателя до точки измерения. Различают элементарные электрический вибратор и магнитную рамку. Электрический вибратор возбуждается источником переменной электродвижу¬щей силы (источником зарядов), магнитная рамка - протекаю¬щей по ней током.

В реальных условиях, с учетом переотражения электромаг¬нитных волн от многочисленных преград (зданий, стен помеще¬ний, автомобилей и т.д.). характер распространения столь сло¬жен, что в общем случае не поддается строгому аналитическому описанию.

В основу методики оценки защищенности основных техни¬ческих средств и систем, предназначенных для обработки, хра¬нения и передачи по линиям связи конфиденциальной информа¬ции, от утечки информации за счет побочных электромагнитных излучений, положен инструментально-расчетный метод опреде¬ления требуемого радиуса контролируемой зоны R2.

Выбор регистрируемых параметров электромагнитного по¬ля ОТСС определяется с учетом особенностей формирования электромагнитного поля в ближней, промежуточной и дальней зонах.

Ближняя зона (зона индукции) простирается на расстояние от ОТСС. равное примерно 1/6 длины волны его ПЭМИ. Даль¬няя зона (волновая) начинается с расстояния, равного примерно 6 длинам волн. Размытая граница между ближней и дальней зонами называется промежуточной (переходной) зоной.

В результате анализа уравнений Максвелла для разных зо¬н были получены следующие выводы:

1. Если в качестве источника поля используется электри¬ческий вибратор, то в ближней зоне преобладает электрическое поле, напряженность Е которого убывает с расстоянием обратно пропорционально кубу расстояния. Магнитное поле имеет меньшую напряженность, но убывающую медленнее - обратно пропорционально квадрату расстояния. При таком характере распространения электромагнитного поля электрического вибратора в переходной зоне значения напряженности электриче¬ской и магнитной составляющих сближаются и в дальней зоне убывают обратно пропорционально расстоянию.

2. Если источником поля является магнитная рамка, то в ближней зоне

напряженность магнитного поля H >> E. В этом случае характер распространения магнитной и электрической составляющих меняется на обратный.

3. Величина связи между электрическими и магнитными компонентами электрического поля определяется соотношением □=E/H, называемым волновым сопротивлением. Волновое со¬противление свободного пространства (в вакууме) в дальней зо¬не постоянно и равно 377 Ом. Так как напряженность электриче¬ского поля, излучаемого электрическим вибратором, в ближней зоне существенно выше напряженности магнитного поля, то □ >> 377 Ом. Поэтому электрическое поле в ближней зоне назы¬вают также высокоимпедансным. В связи с тем, что в ближней зоне напряженность магнитного моля, излучаемого магнитной рамкой, значительно больше напряженности электрического по¬ля, в ней волновое сопротивление много меньше 377 Ом. Такое поле называют низкоимпедансным. Следовательно, при оценке уровней радиосигналов вблизи источников излучения необхо¬димо учитывать существенно более сложный характер распро¬странения электромагнитной волны по сравнению с традицион¬но рассматриваемыми в дальней зоне.

Основным методом предотвращения утечки информации через ПЭМИН является энергетическое скрытие опасного сигна¬ла, которое достигается применением средств пассивной и ак¬тивной зашиты. Опасные сигналы, которые могут содержать конфиденциальную информацию, должны быть ослаблены до уровня, исключающего съем с них информации на границе кон¬тролируемой зоны современными приемниками (пассивная защита - экранирование, фильтрация). К активным средствам за¬щиты относятся всевозможные генераторы шума, обеспечиваю¬щие на границе контролируемой зоны требуемое нормативное отношение сигнал/шум.

3. Описание метода измерений и расчета

3.1. Инструментальная часть метода включает.

Установление режима тестирования для исследуемого ОТСС в соответствии с требовании к тестовым режимам ра¬боты технических средств.

Определение инструментальным путем частотного спектра ПЭМИ исследуемого ОТСС, состоящего из набора спектральных составляющих f1, f2,…, fi,…, fk (где i - натуральные числа от 1 до k: k - число, соответствую-щее полному набору спектральных составляющих).

Определение направления максимального излучения по каж¬дой спектральной составляющей fi ПЭМИ.

Установку антенны измерителя напряженности поля (ИНП) на расстоянии R0 от исследуемого ОТСС (источника излучения). Исходя из требований минимального влия¬ния суммарной погрешности (ошибки в выборе расстоя¬ния) на результат измерений, значение расстояния R0 от исследуемого ОТСС до места установки антенны ИНП рекомендуется принять равным 1м

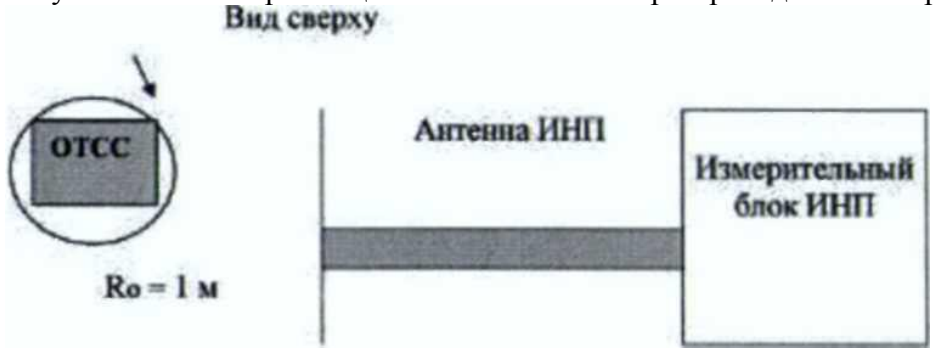
Раздельное измерение в направлении минимального расстоя¬ния до границы контролируемой зоны (КЗ) объекта на¬пряженности электромагнитного поля, возникающей за счет излучения информативного сигнала, по магнитной pHi (в диапазоне частот от 9 кГц до 30 МГц и электри¬ческой Ei (в диапазоне частот от 9 кГц до 1000 МГц) составляющим.

Частотный спектр ПЭМИ исследуемого ОТСС определяют по идентификационным признакам заданного (тестового) режи¬ма его работы. Для определения полного набора информативных составляющих сигналов ПЭМИ антенны ИНП устанавливают на минимальном расстоянии от исследуемого ОТСС. Анализ спек¬тра производят в диапазоне частот от 9 кГц до 1000 МГц. По ре¬зультатам анализа определяют f1, f2,…, fi,…, fk.

Направление максимального ПЭМИ для i-ой спектральной составляющей информативного сигнала определяют в горизон¬тальной плоскости путем поворота ОТСС

на 360 градусов во¬круг своей оси (рис. 1).

Рисунок 1 – Схема размещения ОТСС и ИНП при проведении измерений



Направлением максимального излучения считают направ¬ление, при котором отсчетное устройство ИНП регистрирует максимальное значение измеряемой величины.

В соответствии с инструкцией по эксплуатации применяе¬мого ИНП на частотах f1, f2,…, fi,…, fk измеряются (в дБ) ряды значений напряженности поля pHi в диапазоне частот от 9 кГц до 30 МГц и E, в диапазоне частот от 9 кГц до 1000 МГц, созда¬ваемые информативным сигналом.

При выключенном ОТСС на частотах f1, f2,…, fi,…, fk изме¬ряются ряды значений напряженности поля pHшi и Ешi, созда¬ваемые шумом в месте проведения измерений.

3.2. Расчетная часть метода включает

3.2.1. Расчет расстояний распространения информативного сигнала от ОТСС для его каждой спектральной состав¬ляющей R2i.

3.2.2. Установление требуемого радиуса контролируемой зо¬ны R2 для ОТСС в целом.

3.2.3. Расчеты проводятся по электрической (E) и магнитной (pH) составляющим электромагнитного поля (ЭМП) для каждой спектральной составляющей информативного сигнала.

3.2.4. Порядок проведения расчетов при измеренных значени¬ях напряженности ЭМП по электрическим составляю¬щим E0 и Еш следующий:

- Вычисляется значение напряженности ЭМП по электриче¬ской составляющей Ec, созданная информативным сигна¬лом на частоте f по формуле

$$E_c = \sqrt{E_0^2 - E_ш^2}\ (\text{мкВ/м}), \qquad (1)$$

где E0 - уровень напряженности ЭМП при работе ОТСС в тестируемом режиме;

Еш - уровень шума (напряженность ЭМП при выключен¬ном ОТСС).

- По формулам

$$L_1 = \frac{150}{\pi \cdot f}(\text{м}); \qquad (2)$$

$$L_2 = \frac{1800}{f}(\text{м}) \qquad (3)$$

определяются на частоте f (МГц) границы ближней, промежу¬точной и дальней зон.

- По формуле

$$R = \frac{1}{\sqrt[3]{\frac{K \cdot E_ш}{E_c}}}(\text{м}), \qquad (4)$$

где K = 1 для ОТСС не имеющих в своем составе видеомони¬торов, и K = 0,3 для ОТСС имеющих в своем составе видео¬мониторы, проверяется, достаточно ли уровня чтобы ин¬формативный сигнал от ОТСС распространился за границу ближней зоны.

При рассчитанном R<L1 R принимается за R2.

При R>L1 пересчитывается значение Ес на границу ближ¬ней зоны по формуле

- По формуле

$$E_1 = E_c \cdot (R_0 / L_1)^3 \text{ (мкВ/м).} \qquad (5)$$

проверяется, достаточно ли уровня Е1, чтобы информационный сигнал от ОТСС распространялся за границу промежуточной зоны.

Если R<L2, то информативный сигнал за границу проме¬жуточной зоны не распространяется. В этом случае требуемый радиус контролируемой зоны определяется значением R.

При R>L2 пересчитывается значение Е1 к границе проме¬жуточной и дальней зон - Е2 по формуле

- По формуле

$$R = \frac{L_1}{\sqrt{\frac{K \cdot E_u}{E_c}}} \text{ (м)} \qquad (6)$$

определяется окончательное значение R2 для дальней зоны. Примечание:

1. При условии L1 <1(м) и L2<1(м) в формулах (6) и (8) зна¬чения L1 и L2 принимаются равными 1м, а Е1 и Е2 равными Ес.

2. При расчете возможных расстояний распространения ин-формативного сигнала за счет магнитной составляющей ЭМП в формулы подставляются рН вместо Е.

Величины Е(рН) измеряются в дБ относительно 1 мкВ/м, при расчетах используются значения этих величин в мкВ/м. Перевод выполняется по формулам

4. Условия проведения измерений

Климатические условия должны соответствовать допусти¬мым условиям работы ОТСС и применяемых средств измерений.

5. Подготовка к проведению измерений

5.1. Устанавливают антенну ИНП на расстоянии 1м от ОТСС.

5.2. На ОТСС устанавливают тестовый режим работы.

5.3. Проводят подготовительные работы в соответствии с инст-рукцией по эксплуатации ИНП (присоединение измерительной антенны, выдержка во включенном состоянии, калибровка и т.д.).

2.5 Лабораторная работа № 5 (2 часа).

Тема: «Изучение способов утечки информации по материально-вещественному каналу**»**

2.5.1 Цель работы:

Целью данной лабораторной работы является за¬крепление теоретических знаний и выработка практических на¬выков у студентов при проведении инструментально-расчетной оценки защищенности ОТСС от наводок ПЭМИ на линии и коммуникации, выходящие за пределы контролируемой зоны объекта информатизации.

2.5.2 Задачи работы:

1. Задачей данной лабораторной работы является за¬крепление теоретических знаний и выработка практических на¬выков у студентов при проведении инструментально-расчетной оценки защищенности ОТСС от наводок ПЭМИ на линии и коммуникации, выходящие за пределы контролируемой зоны объекта информатизации.

2.5.3 Перечень приборов, материалов, используемых в лабораторной работе:

1. Персональный компьютер, специальное ПО

2.5.4 Описание (ход) работы:

Теоретическое введение

Работа любого радиоэлектронного средства или электрического прибора всегда сопровождается наличием побочного электромагнитного поля, уровень напряженности которого зависит от многих причин (потребляемой мощности, спектра излучения, условий окружающей среды и т.д.). Помимо того, что само ПЭМИ может быть перехвачено злоумышленником, серьезную угрозу безопасности информации создают наводки ПЭМИ ОТСС на провода и кабели, выходящие за пределы контролируемой зоны (рис. 1).

Когда ток проходит по проводникам первой цепи, вокруг них создается магнитное поле, силовые линии которого пронизывают проводники второй цепи. В результате этого по второй цепи потечет помимо основного еще и переходной ток, создающий помеху основному Защищенность от взаимных помех оценивается так называемым переходным затуханием $Z_{12} = 10lgP_{c1}/P_{u2}$ где P_{c1} и P_{u2} - мощность сигналов в 1-ой цепи и наводки on них во 2-ой цепи. Для надежной защиты информации переходное затухание должно быть не менее величины $10lgP_c/P_{np}$, где P_c и P_{np} - мощность сигнала с информацией и чувствительность приемника злоумышленника, перехватывающего наведенный сигнал. В реальных условиях перехвата данное соотношение не всегда выполняется, поэтому для оценки угрозы безопасности информации существенное значение будет иметь величина погонного затухания наведенного сигнала в линиях и коммуникациях, выходящих за пределы контролируемой зоны объекта информатизации.

Рисунок 1 - Паразитные наводки

3. Описание метода измерений и расчета

3.1. Инструментальная часть метода включает:

3.1.1. Установление режима тестирования для исследуемого ОТСС в соответствии с требованиями к тестовым режимам работы технических средств.

3.1.2. Выбор места проведения измерений.

3.1.3. Проведение поиска компонент тест-сигнала в исследуемой цепи (допускается использование частот, выявленных при инструментальном контроле ПЭМИ данного ОТСС в рамках лабораторной работы № 3).

3.1.4. Измерение напряжения смеси $U_{(c+ш)}$, обнаруженных компонент тест-сигнала и шума.

3.1.5. Измерение уровня шума $U_ш$ в линии на частотах обнаруженных компонент

тест-сигнала.

3.1.6. Определение коэффициента затухания информативного сигнала в исследуемой цепи.

Частотный спектр тест-сигнала исследуемого ОТСС определяется инструментальным путем по идентификационным признакам заданного (тестового) режима его работы. Анализ спектра проводят в диапазоне частот от 0,01 до 250 МГц.

3.2. Расчетная часть метода включает:

3.2.1. Расчет значения напряжения сигнала U_c в точке подсоединения измерительного прибора к линии для каждой частотной компоненты по формуле

$$U_c = 20\lg\sqrt{10^{U(c+ш)/10} - 10^{Uш/10}} \text{ (дБ)}. \qquad (1)$$

3.2.2. Рассчитывается показатель защищенности в точке проведения измерений для каждой из частотных компонент по формуле

$$П = U_c - U_ш \text{ (дБ)}. \qquad (2)$$

3.2.3. Рассчитывается величина коэффициента погонного затухания $K_П$ наведенных сигналов в исследуемой линии для каждой из частот по формуле

$$K_П = \frac{20\lg(U_{1изм}/U_{2изм})}{L} \text{ (дБ/м)}, \qquad (3)$$

где $U_{1изм}$ (мкВ) - напряжение специально созданного сигнала (при помощи генератора сигналов) в точка А (рис. 2);

$U_{2изм}$ (мкВ) - напряжение, измеренное в точке Б;

L (м) - протяженность линии ВТСС между точками А и Б.

3.2.4. Расчет максимальной длины пробега R исследуемой линии для каждой из частот, на которой возможно выделение информативного сигнала, для ОТСС, имеющих в своем составе видеоконтрольные устройства, при нормированном значении отношения сигнал/шум, равном 0,3, проводится по формуле

$$R = \frac{П + 10}{K_П} \text{ (м)}. \qquad (4)$$

Для ОТСС, не имеющих видеоконтрольных устройств, при нормированном значении отношения сигнал/шум, равном единице, проводится по формуле

$$R = \frac{П}{K_П} \text{ (м)}. \qquad (5)$$

3.2.5. Выбирается максимальное из полученных значений R и сравнивается с пробегом линии до границы контролируемой зоны. Если пробег исследуемой линии до границы КЗ больше максимального из всех R, то делается вывод о защищенности информации, обрабатываемой ОТСС, от утечки за счет наводок в исследуемую линию. Если нет, то делается вывод о необходимости принятия дополнительных мер защиты.

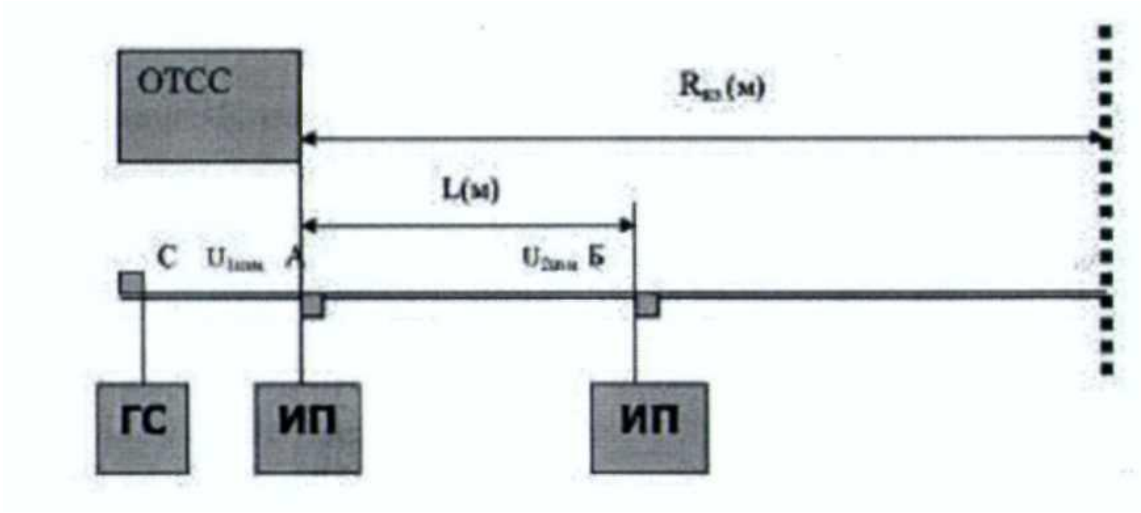


Рисунок 2 - Схема измерении коэффициента погонного затухания:

ГС - высокочастотный генератор сигналов; ИП — измерительный приемник; $R_{кз}$ - радиус контролируемой зоны

4. Условия проведения измерений

4.1. На исследуемых токопроводящих коммуникациях не должно быть высоковольтных напряжений, превышающих предельно допустимые уровни для средств измерений.

4.2. Климатические условия должны соответствовать допустимым условиям работы ОТСС и применяемых средств измерений.

5. Подготовка к выполнению измерений

5.1. На минимальном удалении от исследуемого ОТСС на испытываемой линии выбирается точка подсоединения измерительного пробника с учетом доступности к токопроводящим коммуникациям и обеспечивается в ней надежный электрический контакт с высокочастотным измерительным пробником.

5.2. На ОТСС устанавливается тестовый режим работы.

5.3. Проводятся подготовительные мероприятия в соответствии с инструкциями на применяемые средства измерений (присоединение пробников, выдержка во включенном состоянии, калибровка и т.д.).

6. Выполнение измерений

При выполнении измерений напряжения информативного сигнала, наведенного в токопроводящих коммуникациях, выполняются следующие операции:

6.1. По идентификационным признакам определяется частотный спектр ПЭМИ. Допускается использовать частоты, выявленные при инструментальном контроле ПЭМИ данного ОТСС в рамках лабораторной работы № 3.

6.2. Измеряется напряжение смеси обнаруженных компонент тест-сигнала и шума в соответствии с требованиями инструкций по эксплуатации применяемых средств измерения. Полоса пропускания измерительных приемников выбирается 9 кГц в диапазоне частот от 150 кГц до 30 МГц и 120 кГц в диапазоне от 30 до 250 МГц.

6.3. Производится измерение уровня шума в линии на частотах обнаруженных компонент тест-сигнала при выключенном ОТСС.

6.4. Определяется коэффициент погонного затухания информативного сигнала в исследуемой линии, для чего выполняется следующее:

- собирается схема согласно рис. 2;

- подается сигнал генератора ВЧ в исследуемую линию в точке С, отстоящей от точки А на расстоянии 1-3 м. Подключение генератора рекомендуется осуществлять

индуктивным способом;

- органами управления генератора устанавливается достаточный уровень выходного сигнала (уровень сигнала должен обеспечивать его обнаружение в точках А и Б);

- перестраивая по частоте генератор и измерительный приемник, измеряют на обнаруженных частотах напряжение сигналов генератора в точках А и Б. Точку Б рекомендуется выбирать на расстоянии не менее 10-15 м от точки А.

2.6 Лабораторная работа № 6 (2 часа).

Тема: «Способы и средства защиты информации от наблюдения»

2.6.1 Цель работы:

Изучить средства защиты информации от наблюдения. Проанализировать все имеющиеся способы защиты от наблюдения.

2.6.2 Задачи работы:

1. Способы и принципы работы средств защиты информации от наблюдения.
2. Способы и средства противодействия наблюдению в оптическом диапазоне волн.
3. Способы информационного скрытия объектов от радиолокационного наблюдения.

2.6.3 Перечень приборов, материалов, используемых в лабораторной работе:

1. Персональный компьютер, специальное ПО

2.6.4 Описание (ход) работы:

1.Способы и принципы работы средств защиты информации от наблюдения.

Защита от наблюдения и фотографирования предполагает:

- выбор оптимального расположения средств документирования, размножения и отображения (экраны ПЭВМ, экраны общего пользования и др.) информации с целью исключения прямого или дистанционного наблюдения (фотографирования);
- использование светонепроницаемых стекол, занавесок, драпировок, пленок и других защитных материалов (решетки, ставни и др.);
- выбор помещений, обращенных окнами в безопасные зоны (направления);
- использование средств гашения экранов ЭВМ и табло коллективного пользования после определенного времени работы (работа по режиму времени).

Защита от наблюдения и фотографирования на местности предполагает применение мер маскирования, скрытия объектов в рельефе местности, лесных массивах и, естественно, организацию режима охраны на удалении, обеспечивающего скрытность деятельности.

В более сложных условиях можно применять средства активного маскирования: маскирующие дымы, аэрозоли и другие средства.

2.Способы и средства противодействия наблюдению в оптическом диапазоне волн.

Защита информации от наблюдения в оптическом диапазоне основывается на рассмотренных общих методах с учетом особенностей оптического канала утечки информации. В интересах защиты информации об объекте (его демаскирующих признаков) необходимо уменьшать контраст объект/фон, снижать яркость объекта и не допускать наблюдателя близко к объекту. Мероприятия, направленные на уменьшение величины контраст/фон, называются маскировкой.

Маскировка представляет собой метод информационного скрытия признаков объекта наблюдения путем разрушения его информационного портрета. Применяются следующие способы маскировки:

- использование маскирующих свойств местности;
- маскировочная обработка местности;

- маскировочное окрашивание;
- применение искусственных масок;
- нанесение на объект воздушных пен.

Использование маскирующих свойств местности (неровностей ландшафта, складок местности, холмов, гор, стволов и кроны деревьев и т. д.) является наиболее дешевым способом скрытия объектов. Однако для реализации этого способа необходимо наличие в месте нахождения объекта соответствующих естественных масок. Кроме того, маскирующие возможности растительности зависят от времени года. Эффективность маскировки оценивается отношением площади, закрываемой, например, деревьями к общей площади контролируемой зоны.

Если отсутствуют или недостаточны для маскировки природные условия, то возможна дополнительная обработка местности, повышающая ее маскирующие возможности. Она состоит в дерновании (нарезании дерна) и посеве травы, создании изгородей из живой растительности, в химической обработке участков местности. Обработка местности направлена на изменение фона под основной цвет объекта: на зеленый при дерновании и посеве травы или другой цвет (бурый с различными оттенками, соломенно-желтый) при распятнении.

Распятнение достигается расчисткой поверхности почвы от дерна с помощью машин или химическим путем - солями (железным и медным купоросом, бертолетовой солью и др.) и гербицидами. Этот способ имеет ограниченное применение в связи с большой задержкой проявлений маскировочных свойств местности после обработки и вредным воздействием на природу. Например, трава вырастает через несколько недель после посева, а цвет растительности меняется через несколько дней после химической обработки.

Маскировочное окрашивание осуществляется путем нанесения на поверхность объекта красок, подобранных по цвету и яркости, близкими к фону. Различают 3 вида маскировочного окрашивания:

- защитное;
- деформирующее;
- имитационное.

Защитное окрашивание поверхности объекта проводится одноцветной краской под цвет и среднюю яркость фона окружающей местности и предметов возле маскируемого объекта.

Деформирующее окрашивание предусматривает нанесение на поверхность объекта пятен неправильной геометрической формы 2-3 цветов, имитирующих световые пятна окружающей среды. Деформирующее окрашивание широко применяется для маскировки военной техники и людей в поле-вом обмундировании. Цвет пятен соответствует основным цветам местности, характерным для сезона (лета, зимы).

При имитационном окрашивании цвет и характер пятен на поверхности объекта подбирается под расцветку окружающей местности, объектов или предметов в месте расположения защищаемого объекта. В этом случае обеспечивается наилучшее скрытие.

Маскировочное окрашивание просто реализуется, но эффект маскировки зависит от сезона и иных изменений окружающей среды. Кроме того, часто окрашивание объекта недопустимо.

Для маскировки без окрашивания создаются специальные конструкции - искусственные оптические маски. Они представляют собой металлический или деревянный каркас, накрываемый сплошным или сетчатым (транспарантным) покрытием.

В зависимости от формы маски и способа расположения ее возле объекта различают следующие типы искусственных оптических масок:

- маски-навесы;
- вертикальные маски;
- маски перекрытия;

- наклонные маски;
- радиопрозрачные маски;
- деформирующие маски.

Маски-навесы предназначены для скрытия объектов, расположенных на открытых сверху площадках и защищают их от наблюдения с помощью средств наблюдения, размещаемых на верхних этажах высотных зданий, возвышенностях и горах, на самолетах и космических аппаратах.

Вертикальные маски защищают объекты от наблюдения с земли. Маски перекрытия состоят из каркаса и маскировочного покрытия, которые полностью закрывают объект. Они применяются, прежде всего, для защиты объектов, перевозимых на открытых платформах.

Наклонные маски используются в основном для скрытия теней объемных объектов, по длине которых с учетом положения солнца определяют высоту объектов при наблюдении сверху (с самолетов и космических аппаратов).

Радиопрозрачные маски выполняются из радиопрозрачных материалов (стеклопластика, пенопласта и др.), обычно в форме шара, для скрытия демаскирующих признаков и физической защиты антенн.

Деформирующие маски (обтекатели) не только скрывают внешний вид объекта, но создают у наблюдателя ложное представление о его форме.

Искусственные оптические маски изготовляются в виде различных сборных возимых маскировочных комплектов, которые могут использоваться многократно, не оказывают вредное воздействие на природу, совместимы с другими способами защиты.

Светонепроницаемые одно- и многоцветные воздушные пены, быстро наносимые с помощью пеногенераторов на объекты, обеспечивают их эффективную маскировку в широком диапазоне длин волн в течение до нескольких часов.

Для дезинформирования применяются кроме деформирующих масок ложные сооружения и конструкции, создающие признаки ложного объекта (объекта прикрытия). Ложные сооружения могут быть плоскими и объемными, функциональными и нефункциональными. Они относятся к наиболее до-рогим средствам защиты информации, особенно объемные и функциональные, так как должны воспроизводить полный набор демаскирующих признаков объекта прикрытия в динамике в течение всего периода защиты. Если, например, имитируется объект, на котором работают люди, то они должны убедительно изображать соответствующую деятельность, а не устраивать непрерывные перекуры или греться на солнышке.

Энергетическое скрытие демаскирующих признаков объектов достигается путем уменьшения яркости объекта и фона ниже чувствительности глаза или технического фотоприемника, а также их ослепление. Классическим примером ослепления может служить применение наступающими совет-скими войсками ночью в Берлинской операции 1945 г. 142 прожекторов, свет которых лишил фашистов возможности вести наблюдение и эффективно обороняться. Наиболее естественным способом энергетического скрытия является проведение мероприятий, требующих защиты информации о них, ночью. Яркость объектов, имеющих искусственные источники света, снижается путем их выключения или экранирования светонепроницаемыми шторами и экранами.

Энергетическое скрытие объектов, наблюдаемых в отраженном свете, обеспечивают рассмотренные искусственные маски, а также естественные и искусственные аэрозоли в среде распространения.

Аэрозоли - вещества в виде дисперсии твердых частиц и капель жидкости, находящиеся во взвешенном состоянии в воздухе. К аэрозолям относятся обычно дымы, туманы, пыль, смог.

Естественные аэрозоли образуются обычно пылью и частицами воды. В зависимости от размеров частиц воды метеорологическая дальность принимает значения от десятков метров (при очень сильном тумане, дожде и снеге) до 10-20 км (при дымке).

Хорошая видимость обеспечивается при дальности 20-50 км, а исключительно хорошая - более 50 км.

Наиболее распространенной разновидностью аэрозольного состояния атмосферы является дымка. Дымка возникает при слипании мелкодисперсных частиц воздуха друг с другом и взаимодействии их с атмосферной влагой. В условиях повышенной влажности воздуха в результате взаимодействия паров воды с частицами растворимых в ней солей образуется туманная дымка, при которой метеорологическая дальность составляет 1-10 км.

Влияние аэрозольных образований в общем случае проявляется как в рассеянии, так и поглощении света частицами аэрозоля. Коэффициент ослабления (поглощения) в видимой области спектра изменяется в 1.5-2 раза. С увеличением длины волны потери ослабевают. Потери энергии волны при λ=0.55 мкм приблизительно в 10 раз больше потерь для λ=1.06 мкм. Аэрозольное рассеяние света зависит от коэффициентов его ослабления отдельными частицами, их концентрации и размеров. Оно определяет прозрачность и метеорологическую дальность видимости.

Использование естественных аэрозолей в качестве средств защиты от наблюдения затруднено из-за случайного характера их проявлений в виде образований, приводящих к малой метеорологической дальности. Тем не менее, естественные аэрозоли в виде облаков создают серьезные проблемы для раз-ведки при наблюдении наземных и надводных объектов с помощью средств космической разведки. Учитывая, что траектории движения КА и облаков независимые, то вероятность выполнения временного условия разведывательного контакта (совпадения моментов пролета спутника над интересующим разведку объектом и отсутствием облачности) равна произведению вероятностей каждого из этих событий. Следовательно, для обнаружения и распознавания объекта даже при отсутствии мер защиты информации о нем потребуются многократные пролеты над ним разведывательных КА.

С помощью дымовых шашек, специальных боеприпасов (снарядов, бомб), аэрозольных генераторов и дымовых машин создаются дымовые завесы (облака) из искусственных аэрозолей, обеспечивающие (при учете направления и силы ветра), эффективное, но кратковременное скрытие. Время и площадь скрытия зависит от многих факторов, в том числе от объема облака дыма, направления и скорости ветра, и колеблется от минут до 1-2-х часов. Наиболее эффективные завесы образуются при скорости ветра 3-5 м/с.

В качестве химических веществ для образования дыма применяются эпоксидные, фенольные, полиэтиленовые, силикатные, уретановые смолы и другие высокомолекулярные соединения. Дымы из таких веществ получаются распылением частиц вещества в потоке горячих газов и другими способа-ми. 13 зависимости от состава компонентов частицы, образующие аэрозольное облако, могут иметь диаметр от 1 до 100 мкм. Для образования аэрозольного облака, обеспечивающего, например, ослабление излучений в ИК-диапазоне примерно в 80 раз, на площади 600 м2 потребуется распылить около 400 г дымообразующего вещества [41].

Так как спектральные характеристики объектов и среды отличаются для видимого и ИК-диапазонов, то при организации защиты информации от наблюдения в оптическом канале необходимо учитывать диапазон частот носителя информации. Хотя параметры средств визуально-оптического наблюдения (по разрешению, дальности, цвету изображения) в ИК-диапазоне значительно более низкие, чем в видимом, но при наблюдении в нем появляется дополнительный демаскирующий признак объектов, не обнаруживаемый в видимом, - температура поверхности объекта относительно температуры фона.

Естественный фон в ИК-диапазоне можно рассматривать как сложный источник ИК-излучения, характеристики которых зависят от условий освещения, географической широты и долготы, сезона и температуры среды, метеоусловий, природы подстилающей

поверхности, времени и т. п. Отражающая способность ряда природных фонов, таких как трава и листва деревьев, возрастает со смещением максимума излучений в область более длинных волн. Например, отражающая способность травы и листвы в диапазоне волн 0.76-12 мкм выше отражающей способности в видимом диапазоне приблизи-тельно в 5-10 раз, коры — в 3-5 раз. Поэтому объекты, окрашенные маскирующей краской для видимого диапазона, могут хорошо наблюдаться в ИК-диапазоне. Следовательно, при выборе краски необходимо учитывать характер изменения ее коэффициента отражения от длины волны падающего на объект света, в том числе и в ИК-диапазоне.

Кроме того, на яркость объекта с собственными источниками тепла, и, следовательно, на его контраст с фоном в ИК-диапазоне влияет температура поверхности объекта. Для его информационной защиты применяются различные теплоизолирующие экраны, в том числе листья деревьев и кустарников, сено, брезент и др. материалы. Хорошими теплоизолирующими свойствами обладают воздушные пены.Для экранирования объектов наблюдения в помещении применяются шторы, занавески, жалюзи, тонированные стекла и пленки. Эффективные экраны создают жалюзи. По виду материалов жалюзи делятся на тканевые, пластиковые, деревянные и металлические. Лучшие эксплуатационные свойства имеют деревянные и металлические жалюзи. По расположению ламелей жалюзи бывают вертикальные, горизонтальные и рулонные.

3. Способы информационного скрытия объектов от радиолокационного наблюдения.

Специфика защиты от радиолокационного наблюдения вызвана особенностями получения радиолокационного изображения. Структура радиолокационного изображения зависит от разрешающей способности радиолокатора, электрических свойств отражающей поверхности объектов и фона, от степени ее неровностей (шероховатости), от длины и поляризации волны, облучающей объект, угла падения электромагнитных волн на поверхность объекта. Разрешающая способность локатора определяется в основном шириной диаграммы направленности его антенны, как известно, совмещающей в одной конструкции функции, передающей и приемной.

В настоящее время наиболее широко используется для радиолокации см-диапазон. Разрешение на местности в этом диапазоне самолетных (бортовых) радиолокаторов составляет единицы метров. С целью повышения разрешающей способности радиолокаторов применяется мм-диапазон, в котором проще создать антенны приемлемых размеров с более узкой диаграммой направленности. Но мм-волны сильнее затухают в атмосфере, что приводит к снижению дальности наблюдения. Кроме того, более длинные волны имеют лучшую проникающую способность в поверхность объекта, что затрудняет его маскировку.

Таким образом, радиолокационное изображение существенно отличается от изображения в оптическом диапазоне и используется разведкой для получения дополнительных демаскирующих признаков на существенно большем удалении от объекта и в неблагоприятных климатических условиях. Указанные особенностей учитываются при организации защиты информации. Меры по защите направлены на снижение ЭПР объекта в целом и его характерных участков, содержащих информативные демаскирующие признакию

Информационное скрытие обеспечивается в результате разрушения структуры «блестящих точек» на экране локатора путем покрытия объекта радиотражающими оболочками и экранами с иной конфигурацией, размещения в месте расположения объекта дополнительных отражателей и генериро-вания радиопомех.

В качестве дополнительных радиоотражателей применяются уголковые, линзовые, дипольные отражатели и переизлучающие антенные решетки (ПАР).

Уголковый радиоотражатель состоит из жестко связанных между собой взаимно перпендикулярных плоскостей (см. рис. 3.1).

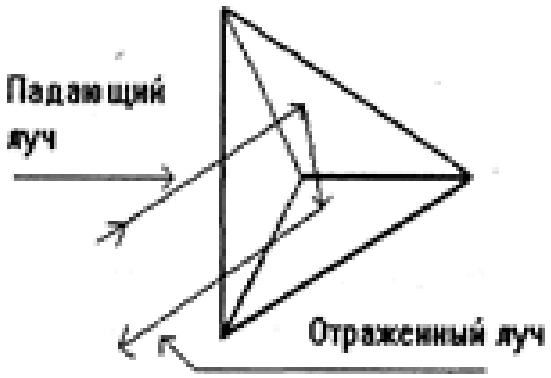


Рисунок 3.1 - Схема уголкового отражателя

Важнейшим свойством уголковых отражателей является то, что значительная доля энергии волны, падающей на них с любого направления в пределах достаточно большого угла (около 80 градусов), отражается обратно в сторону облучающей РЛС. Благодаря этому уголковые радиоотражатели даже небольших размеров имеют значительную эффективную площадь рассеяния. Например, ЭПР трехгранного уголкового отражателя с размерами граней 0.5 м и длине волны РЛС 3 см составляет 290 м2, в то время как ЭПР самолета-бомбардировщика В-52 - около 100 м2.

Линзовые отражатели создаются на основе линз Люнеберга. Линза представляет собой многослойный шар с различными значениями диэлектрической проницаемости слоев (рис. 3.2).

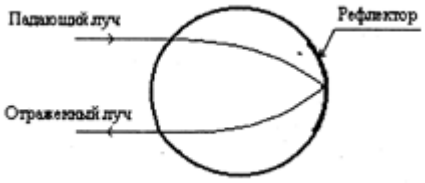


Рисунок 3.2 - Схема линзы Люнеберга

При такой конструкции электромагнитные волны фокусируются на внутренней поверхности шара, покрытой металлической радиоотражательной пленкой-экраном. Ширина диаграммы рассеяния линзы зависит от размеров экранирующей поверхности сферы и достигает 140 градусов. ЭПР линзового отражателя диаметром 60 см и массой 40 кг достигает на длине волны λ=10 см величины более 150 м2, на λ=3 см более 1800 м2.

Переизлучающие антенные решетки (ПАР) состоят из набора обычных антенн, которые работают в режиме переизлучения принимаемых сигналов. Такой режим достигается путем замыкания антенн в точке подключения фидера или волновода. Простейшие ПАР образуются при попарном соединении элементарных полуволновых вибраторов,

Уголковые радиоотражатели, линзы Люнеберга, ПАР, размещенные вблизи защищаемого объекта, создают на экране РЛС многочисленные яркие засветки, среди которых трудно обнаружить маскируемый объект.

Для маскировки воздушных объектов применяют дипольные радиоотражатели (диполи). Они представляют собой полоски металлизированной бумаги или алюминиевой фольги, металлизированные стеклянные или нейлоновые волокна, разбрасываемые в зоне расположения защищаемого объекта. Длина диполей и их толщина выбираются так, чтобы обеспечить эффективное рассеивание радиоволн по возможности в более широком диапазоне частот. Диполи в виде металлизированных стекловолокон имеют длину 35-40 см и толщину 0.025 мм, медная проволока толщиной в доли мм нарезается длиной около 50 см. Дипольные отражатели обычно упаковываются в пачки из десятков и сотен тысяч единиц и при выбрасывании с самолета в воздух создают облако медленно опускающихся

на землю отражателей. Отраженные от них сигналы наблюдаются на экране индикатора РЛС в виде множества ярких точек, маскирующих отраженный от самолета сигнал. Если последовательно сбрасывать достаточно большое количество, пачек, то на экране РЛС образуются засвеченные полосы, в которых трудно обнаруживать воздушные объекты.

Энергетическое скрытие достигается за счет уменьшения эффективной площади рассеяния объекта в основном двумя способами: изменением диаграммы направленности отражающей поверхности объекта и поглощением облучающей энергии РЛС. Уменьшение отраженной энергии для объекта, подлежащего защите от радиолокационного наблюдения, должно предусматриваться еще при его создании путем исключения на поверхности объекта плоскостей, образующих уголковые отражатели.

ЭПР конусообразных и шарообразных форм в сотни раз меньше уголковых отражателей. Готовые изделия, имеющие поверхности сложной формы с резкими переходами, целесообразно накрывать экранами, искажающими и отклоняющими диаграмму направленности объектов, лучше всего шарооб-разной формы.

Для энергетического скрытия объектов от радиолокационного наблюдения его поверхность покрывают также материалами, обеспечивающими градиентное и интерференционное поглощение облучающей электромагнитной энергии.

Градиентное поглощение обеспечивают многослойные материалы, каждый слой которых состоит из основы - диэлектрика (стеклотекстолита, пенопласта, каучука и др.) и наполнителя (ферритов, карбонильного железа, порошка графита, угольной пыли и др.), поглощающих (электромагнитную энергию. Внешний слой поглотителя имеет диэлектрическую проницательность, близкую к 1, а для увеличения поверхности имеет рифленую структуру или шипы. В каждом последующем слое диэлектрическая проницаемость увеличивается. По мере проникновения электромагнитной волны в поглощающий материал ее энергия убывает, а направление изменяется. В результате искривления направления распространения волны удлиняется ее путь в поглощающем материале и, следовательно, увеличивается поглощение. Например, покрытие из пористого стекловолокна толщиной 12.7 мм поглощает до 99% энергии электромагнитной поля в см-диапазоне длин волн.

Другой вид радиопоглощающего материала использует эффект интерференции прямой (падающей) и отраженной от объекта электромагнитных волн. Простейший поглощающий материал состоит из слоя диэлектрика и электропроводящей пленки. В результате наложения прямой и отраженной волн в диэлектрике возникают стоячие волны.Тип и толщина диэлектрика, магнитная проницаемость и волновое сопротивление пленки выбираются такими, чтобы сдвиг по фазе между падающей и отраженной волнами был близок к 180°. В этом случае происходит подавление отраженной волны падающей и ЭПР объекта резко уменьшается. Однако такой эффект наблюдается в узком диапазоне длин волн. Для расширения диапазона применяются многослойные материалы, каждый слой которых рассчитан на свой диапазон длин волн облучающей электромагнитной волны. Но многослойные материалы, обеспечивающие эффективное поглощение в достаточно широком диапазоне частот, толстые и тяжелые.

В современных поглощающих материалах используют оба способа уменьшения энергии отраженной электромагнитной волны. Например, коэффициент отражения керамического ферритового радиопоглощающего материала составляет 10% в диапазоне волн 30-300 МГц при толщине феррито-вого слоя 0.83 см. Созданы достаточно легкие радиопоглощающие материалы в виде многослойной ткани.

Примером технических решений, обеспечивающих эффективное энергетическое скрытие за счет соответствующей конструкции с плавными формами и применения поглощающих материалов, является американская технология «Стелс». На ее основе созданы самолеты-бомбардировщики В-1 и В-2, эффективная площадь рассеяния которых не превышает ЭПР автомобиля.

Другой способ энергетического скрытия, который широко применяется для защиты

объектов от радиолокационного наблюдения, - генерация помех. Простейшей помехой является гармоническое колебание на частоте РЛС, создаваемое генератором помех в месте нахождения защищаемого объекта. Так как диаграмма направленности антенны РЛС имеет, как правило, боковые лепестки, то такая помеха создает шумовую засветку экрана локатора.

Более сложной по структуре является модулированная помеха с одним или несколькими изменяющимися параметрами. Модулированная помеха бывает непрерывной и импульсной и обладает спектром, близким к спектру излучения РЛС. По эффекту воздействие помехи классифицируются на маскирующие изображение объекта путем зашумления экрана РЛС и имитирующие на нем ложные световые пятна. Изменяя структуру и время задержки имитационной помехи можно менять форму, место и характер движения ложной засветки на экране локатора.

Защита информации об объектах, находящихся в воде, предусматривает, прежде всего, защиту от гидроакустического наблюдения. Способы этой защиты по сути соответствуют рассмотренным с учетом особенностей канала утечки. В качестве основных применяются следующие:

- маскировка с использованием природных явлений. При перепаде температуры слоев возникают акустические экраны, трудно преодолимые для акустических излучений;
- использование звукопоглощающих покрытий сотовой конструкции из нейлона, полиэтилена, полипропилена и различных пластмасс, а также содержащих натуральный каучук. За рубежом проводятся опыты по покрытию корпусов подводных лодок материалами, поглощающими до 90% акустической энергии;
- создание активных помех гидролокаторам, в том числе путем ретрансляции облучающих сигналов с усилением их мощности.

2.7 Лабораторная работа № 7 (2 часа).

Тема: «Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами»

2.7.1 Цель работы: изучить существующие способы защиты информации, обрабатываемой СВТ и АС.

2.7.2 Задачи работы:

1. Классификация объектов информатизации.
2. Экранирование технических средств их соединительных линий.
3. Экранированные помещения.
4. Заземление технических средств.

2.7.3 Перечень приборов, материалов, используемых в лабораторной работе:

1. Персональный компьютер, специальное ПО

2.7.4 Описание (ход) работы:

Под **объектами информатизации, аттестуемыми по требованиям безопасности информации**, понимаются автоматизированные системы различного уровня и назначения, системы связи, отображения и размножения вместе с помещениями, в которых они установлены, предназначенные для обработки и передачи информации, подлежащей защите, а также сами помещения, предназначенные для ведения конфиденциальных переговоров.

Защищаемыми объектами *информатизации* в соответствии с СТР-К являются:

- средства и системы *информатизации* (средства вычислительной техники, автоматизированные системы различного уровня и назначения на базе средств вычислительной техники, в том числе информационно-вычислительные комплексы, сети и системы, средства и системы связи и передачи данных, технические средства приема,

передачи и обработки информации (телефонии, звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео и буквенно-*цифровой информации*), программные средства (операционные системы, *системы управления базами данных*, другое общесистемное и прикладное программное обеспечение), используемые для обработки конфиденциальной информации;

- технические средства и системы, не обрабатывающие непосредственно конфиденциальную информацию, но размещенные в помещениях, где она обрабатывается (циркулирует);
- защищаемые помещения.

Объект защиты информации - информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации.

В соответствии с данным определением можно классифицировать объекты защиты в соответствии с рисунком 8.1.

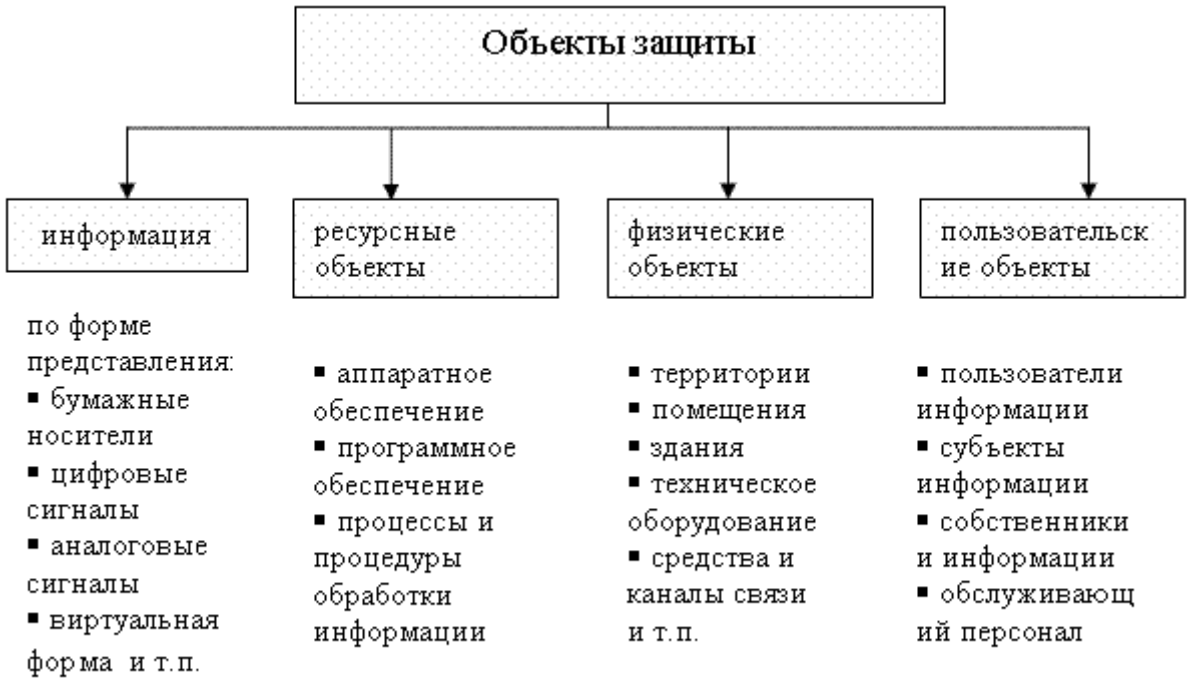


Рисунок 2.1 - Классификация объектов защиты

Методы и способы защиты объектов информатизации зависят от конкретных требований и условий, предъявляемых к этим объектам.

1. Экранирование технических средств их соединительных линий.

С целью уменьшения уровня побочных электромагнитных излучений, средства обработки информации ограниченного доступа выпускаются в специальном защищённом исполнении.

В качестве примера, на рис. 2.2 представлена ПЭВМ, выполненная в специальном экранированном корпусе.

Наряду с техническими средствами экранированию подлежат монтажные провода и соединительные линии.

Чтобы уменьшить уровень ПЭМИ, необходимо особенно тщательно выполнять соединение оболочки провода (экрана) с корпусом аппаратуры. Подключение оболочки

должно осуществляться путём непосредственного контакта (лучше всего путём пайки или сварки) с корпусом.

Вместе с тем соединение оболочки провода с корпусом в одной точке не ослабляет в окружающем пространстве магнитное поле, создаваемое протекающим по проводу током. Для экранирования магнитного поля необходимо создать поле такой же величины и обратного направления. С этой целью необходимо весь обратный ток экранируемой цепи направить через экранирующую оплётку провода. Для полного осуществления этого принципа необходимо, чтобы экранирующая оболочка была единственным путём для протекания обратного тока.

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

На низких частотах приходится использовать более сложные схемы экранирования - коаксиальные кабели с двойной оплёткой.

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

Применение экранирующей оболочки существенно увеличивает ёмкость между проводом и корпусом, что в большинстве случаев нежелательно. Экранированные провода более громоздки и неудобны при монтаже, требуют предохранения от случайных соединений с посторонними элементами и конструкциями.

Длина экранированного монтажного провода должна быть меньше четверти длины самой короткой волны передаваемого по проводу спектра сигнала. При использовании более длинных участков экранированных проводов необходимо иметь в виду, что в этом случае экранированный провод следует рассматривать как длинную линию, которая во избежание искажений формы передаваемого сигнала должна быть нагружена на сопротивление, равное волновому.

Для уменьшения взаимного влияния монтажных цепей следует выбирать длину монтажных высокочастотных проводов наименьшей, для чего элементы высокочастотных схем, связанные между собой, следует располагать в непосредственной близости, а неэкранированные провода высокочастотных цепей - при пересечении под прямым углом. При параллельном расположении такие провода должны быть максимально удалены друг от друга или разделены экранами, в качестве которых могут быть использованы несущие конструкции электронной аппаратуры (кожух, панель и т.д.).

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

Кабельные экраны выполняются или в форме цилиндра из сплошных оболочек, или в виде спирально намотанной на кабель плоской ленты, или в виде оплётки из тонкой проволоки. Экраны при этом могут быть однослойными, многослойными и комбинированными, изготовленными из свинца, меди, стали, алюминия и их сочетаний (алюминий-свинец, алюминий-сталь, медь-сталь-медь и т.д.).

В кабелях с наружными пластмассовыми оболочками применяют экраны ленточного типа в основном из алюминиевых, медных и стальных лент, накладываемых спирально или продольно вдоль кабеля.

В области низких частот корпуса применяемых многоштырьковых низкочастотных разъёмов являются экранами и должны иметь надёжный электрический контакт с общей шиной или землёй прибора, а зазоры между разъёмом и корпусом должны быть закрыты электромагнитными уплотняющими прокладками. В области высоких частот коаксиальные кабели должны быть согласованы по волновому сопротивлению с используемыми высокочастотными разъёмами. При заделке коаксиального кабеля в высокочастотные разъёмы жила кабеля не должна иметь натяжения в месте соединения с контактом разъёма, а сам кабель должен быть жёстко прикреплён к шасси аппаратуры

вблизи разъёма.

Наиболее экономичным способом экранирования информационных линий связи между устройствами ТСОИ считается групповое размещение их информационных кабелей в экранирующий распределительный короб. Когда такого короба не имеется, то приходится экранировать отдельные линии связи.

Для защиты линии связи от наводок необходимо разместить её в экранирующую оплётку или фольгу, заземлённую в одном месте, чтобы избежать протекания по экрану токов, вызванных неэквипотенциальностью точек заземления.

Для защиты линии связи от наводок необходимо минимизировать площадь контура, образованного прямым и обратным проводами линии. Если линия представляет собой одиночный провод, а возвратный ток течёт по некоторой заземляющей поверхности, то необходимо максимально приблизить провод к поверхности. Если линия образована двумя проводами, то их необходимо скрутить, образовав бифиляр (витую пару). Линии, выполненные из экранированного провода или коаксиального кабеля, в которых по оплётке протекает возвратный ток, также отвечают требованию минимизации площади контура линии.

Рисунок 2.2 - ПЭВМ«ЕС1855.М.02» в специальном защищенном исполнении

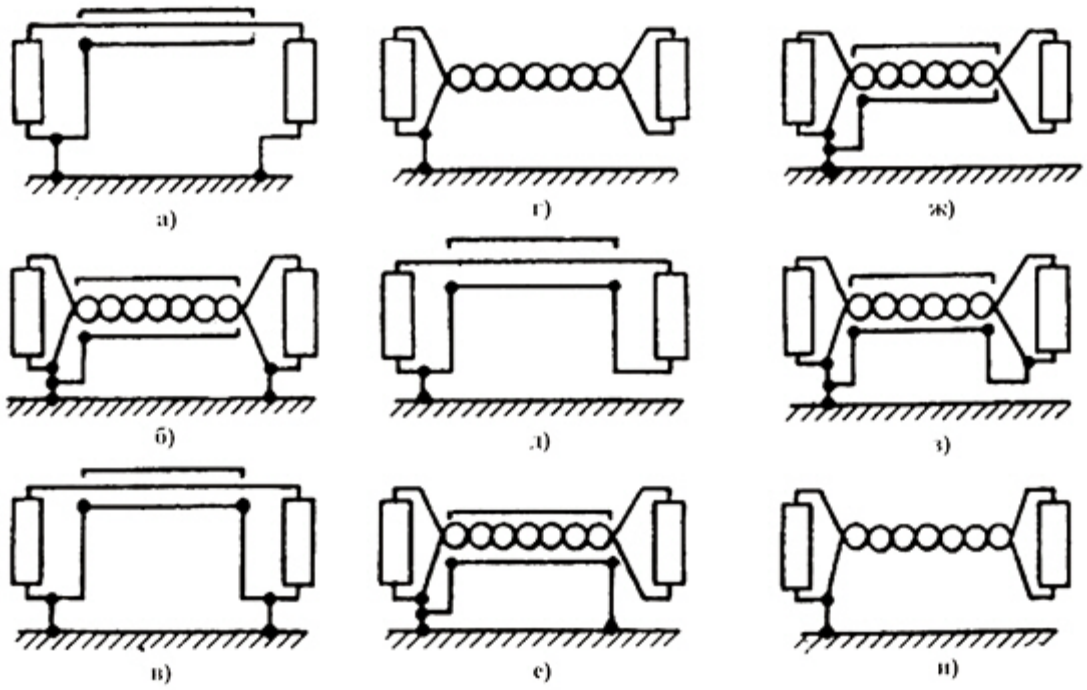


Рисунок 2.3 - Сравнение защищённости различных цепей от влияния внешних магнитных и электрических полей:

а) 0 дБ;
б) 2 дБ;
в) 5 дБ;
г) 49 дБ, скрученная пара, 18 витков на метр;
д) 57 дБ;
е) 64 дБ, схема предпочтительна на высоких частотах;
ж)64 дБ;
з) 71 дБ;
и) 79 дБ, скрученная пара (54 витка на метр).

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

Приведём несколько схем, используемых на частотах порядка 100 кГц.

Цепь, показанная на рис. 2.3 (а), имеет большую площадь петли, образованной «прямым» проводом и «землёй». Эта цепь подвержена прежде всего магнитному влиянию. Экран заземлён на одном конце и не защищает от магнитного влияния. Переходное затухание для этой схемы примем равным 0 дБ для сравнения с затуханием схем на рис. 2.3 (б - и).

Схема на рис. 2.3(б) практически не уменьшает магнитную связь, так как обратный провод заземлён с обоих концов, и в этом смысле она аналогична схеме на рис. 2.3 (а). Степень улучшения соизмерима с погрешностью расчёта (измерения).

Схема на рис. 2.3 (в) отличается от схемы на рис. 2.3(а) наличием обратного провода -коаксиального экрана, однако экранирование магнитного поля ухудшено, так как цепь заземлена на обоих концах, в результате чего с «землёй» образуется петля большой площади.

Схема на рис. 2.3 (г) позволяет существенно повысить защищённость цепи благодаря скрутке проводов. В этом случае (по сравнению со схемой на рис. 2.3 (б)) петли нет, поскольку правый конец цепи не заземлен.

Дальнейшее повышение защищённости цепи достигается применением схемы на рис. 2.3 (с), коаксиальная цепь которой обеспечивает лучшее магнитное экранирование, чем скрученная пара на рис. 2.3 (г).

Площадь петли в схеме на рис. 2.3 (д) не больше, чем в схеме на рис. 2.3 (г), так как продольная ось экрана коаксиального кабеля совпадает с его центральным проводом.

Таблица 2.1 - Степень экранирующего действия различных типов зданий

Тип здания	**Степень экранирования, дБ**		
	100 МГц	**500 МГц**	**1000 МГц**
Оконный проём 30 % от площади стены			
Кирпичное здание с толщиной стен 1,5 кирпича	13-15	15-17	16-19
Железобетонное здание с ячейкой арматуры 15 х15 см и толщиной стен 160 мм	20-25	18-19	15-17
Оконный проём 30 % от площади стены, закрытый металлической решёткой с ячейкой 5 х 5 см			

Кирпичное здание с толщиной стен 1,5 кирпича	17-19	20-22	22-25
Железобетонное здание с ячейкой арматуры 15 х15 см и толщиной стен 160 мм	28-32	23-27	20-25

Схема на рис. 2.3 (е) позволяет повысить защищённость цепи благодаря тому, что скрученная пара заземлена лишь на одном конце. Кроме того, в этой схеме используется независимый экран.

Схема на рис. 2.3 (ж) имеет ту же защищённость, что и схема на рис. 2.3 (е): эффект тот же, что и при заземлении на обоих концах, поскольку длина цепи и экрана существенно меньше рабочей длины волны.

Причины улучшения защищённости схемы на рис. 2.3(з) по сравнению с рис. 2.3 (ж) объяснить трудно. Возможной причиной может быть уменьшение площади эквивалентной петли.

Более плотная скрутка проводов (схема рис. 2.3 (и)) позволяет дополнительно уменьшить магнитную связь. Кроме того, при этом уменьшается и электрическая связь (в обоих проводах токи наводятся одинаково).

Для уменьшения магнитной и электрической связи между проводами необходимо максимально их разнести и максимально уменьшить длину их параллельного пробега.

При нулевых уровнях сигналов (0 dB) в соединительных линиях ТСОИ между ними и посторонними проводниками должно обеспечиваться переходное затухание не менее 114 dB (13 Нп). Данное переходное затухание обеспечивается, как правило, при прокладке кабелей ТСОИ на расстоянии не менее 0,1 м от посторонних проводников. При этом допускается прокладка кабелей ТСОИ вплотную с посторонними проводниками при суммарной длине их совместного пробега не более 70 м.

2. Экранированные помещения.

В обычных (неэкранированных) помещениях основной экранирующий эффект обеспечивают железобетонные стены домов (табл. 2.2).

Как правило, степень экранирования обычных помещений невысока вследствие наличия в них окон, дверей и вентиляционных отверстий, поэтому их экранированию необходимо уделять первостепенное внимание.

Таблица 2.2. - Предельно достижимые величины ослабления электромагнитных излучений для различных типов экранирующих помещений

Тип конструкции экранированного помещения	**Степень экранирования, дБ**
Одиночный экран из сетки; одиночная экранированная дверь, оборудованная зажимными устройствами; внутренние рольставни на окно; специальные электрические фильтры; экранирующие фильтры для притока и вытяжки (вентиляционные).	40
Одиночный экран из металлизированной ткани; одиночная экранированная дверь, оборудованная зажимными устройствами; экранированное окно с экранированным стеклом, внутренние рольставни на окно; специальные электрические фильтры; экранирующие фильтры для притока и вытяжки (вентиляционные).	60
Двойной экран из сетки или металлизированной ткани; двойная экранированная дверью-тамбуром и зажимными устройствами конструкция; специальные электрические фильтры; экранирующие фильтры для притока и вытяжки (вентиляционные).	80
Сплошной стальной экран; пневматическая экранированная дверь; специальные электрические фильтры; экранирующие фильтры	100

для притока и вытяжки (вентиляционные).	

Для экранирования дверей в основном используется листовая сталь, а на окна устанавливается одно или двухслойная медная сетка с ячейкой не более 2х2 мм, причём расстояние между слоями сетки должно быть не менее 50 мм. Сетки удобнее делать съёмными в металлическом обрамлении.

В экранированных помещениях также могут устанавливаться оконные металлизированные рамы со стёклами, на которые нанесено специальное токопроводящее покрытие. Эффективность экранирования у таких стёкол в радиодиапазоне составляет около 30 дБ.

Для повышения эффективности экранирования могут использоваться шторы из металлизированной ткани.

Для повышения качества экранирования вентиляционных отверстий в них устанавливают экраны, представляющие собой сотовые конструкции, закрывающие вентиляционное отверстие, с прямоугольными, круглыми, шестигранными ячейками. Для достижения эффективного экранирования размеры ячеек должны быть менее одной десятой от длины волны.

При необходимости повышения экранирования помещения более чем на 20-25 дБ необходимо дополнительно экранировать не только двери, но и ограждающие конструкции (стены, пол, потолок), а также устанавливать на окна рольставни. Такие помещения уже можно называть экранированными.

Степень экранирования помещения зависит от используемых средств экранирования и может составлять от 40 до 60 дБ при наличии окон в помещении и до 100 дБ при их отсутствии.

На практике экранировку электромагнитных волн более 60 дБ можно обеспечить только в специальных экранированных сооружениях (ЭС) или в экранированных камерах (ЭК).

Выполняются экранированные сооружения из стальных сплошных листов, соединённых электродуговой сваркой.

Экранированное сооружение обеспечивает затухание электромагнитной энергии 60-120 дБ в диапазоне частот от 10 кГц до 37500 МГц и более.

В экранированных сооружениях (камерах) устанавливаются экранированные двери, технологические проёмы, системы контроля и сигнализации экранированных дверей, фильтры помехоподавляющие (электрические, воздуховодные, трубопроводные, световые, телекоммутационные), системы вентиляции и кондиционирования, системы пожарной сигнализации, дымоудаления и автоматического пожаротушения (рис. 2.4).

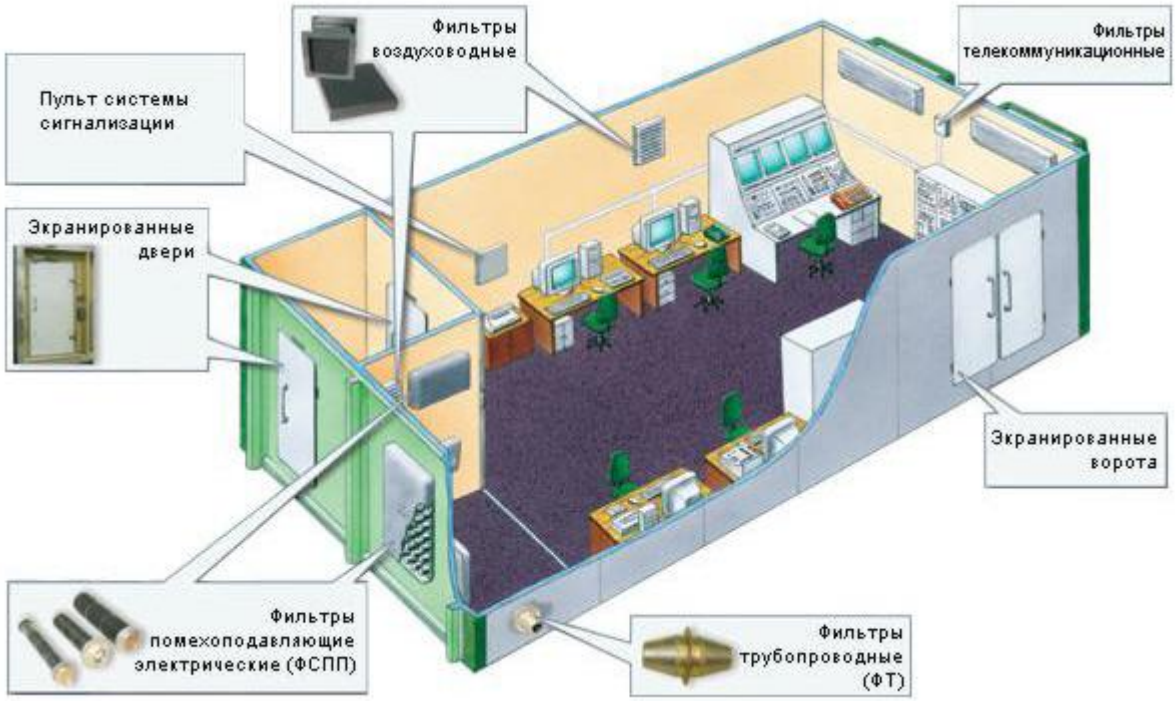


Рисунок 2.4 - Схема экранированного сооружения

Экранированные двери предназначены для организации оперативного входа-выхода обслуживающего персонала в экранированное сооружение. Они имеют контактное магнитное уплотнение и в них отсутствуют механические запоры и прижимы, что обеспечивает безопасность прохода в экстремальных условиях.

При закрытии экранированной двери должен обеспечиваться надёжный электрический контакт со стенками помещения (с дверной рамой) по всему периметру.

Стандартные размеры дверей составляют 900х2000 мм и 1500х2000 мм. Установка нескольких дверей через систему тамбуров в комплекте с системой сигнализации обеспечивает проход персонала без нарушения защитных функций экранированного помещения.

Экранированные ворота предназначены для оперативного ввоза-вывоза крупногабаритного оборудования в экранированное сооружение.

Системы сигнализации и контроля экранированных дверей и ворот предназначены для контроля их положения, световой и звуковой сигнализации при нарушении экранировки и для разрешения или запрещения прохода персонала в экранированное помещение в зависимости от положения дверей.

а) *б)* *в)*

Рисунок 2.5 - Экранированные двери: а) без тамбура; б) и в) с тамбуром

Фильтры помехоподавляющие электрические (рис. 2.6) предназначены для подавления побочных электромагнитных излучений и наводок (ПЭМИН) в цепях электропитания и сигнализации, а также организации ввода этих цепей в защищаемые и экранированные сооружения и помещения.

а) ***б)***

Рисунок 2.6 - Фильтры помехоподавляющие электрические:

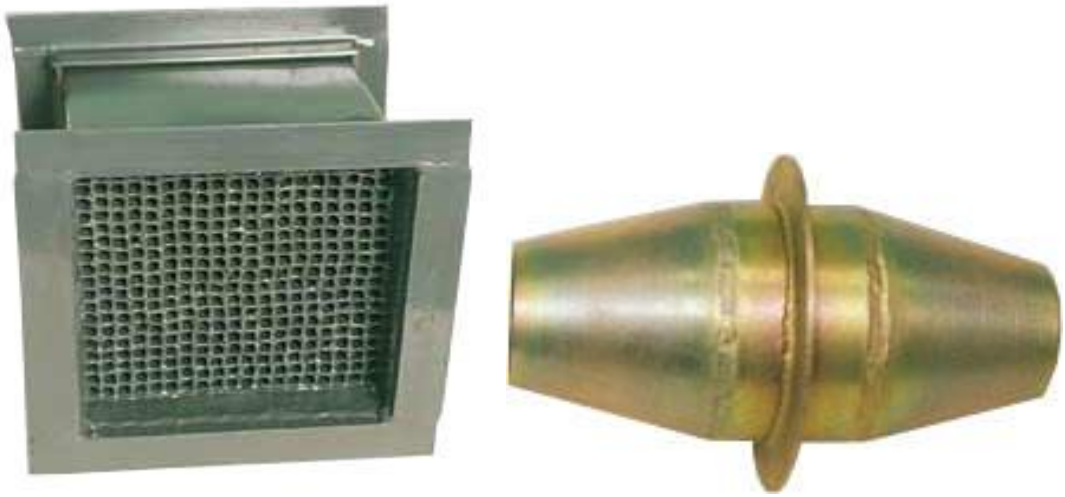
а) типа ФП (индуктивно-ёмкостные многопроводные);

б) типа ФСПП (на основе электродинамических замедляющих структур, однопроводные и многопроводные)

Фильтры воздуховодные (рис.2.7 а) предназначены для воздухообмена внутреннего

объёма экранированного сооружения с внешней средой в целях жизнеобеспечения обслуживающего персонала и дымоудаления, а также ввода световолоконных кабелей. Фильтры трубопроводные (рис. 2.7 б) предназначены для подачи в экранированные сооружения жидкостей и газов.

Фильтры телекоммуникационные предназначены для ввода в экранированные камеры цифровых кодовых сигналов без нарушения экранирующих характеристик сооружения.



а) ***б)***

Рисунок 2.7 - Фильтры: воздуховодный (а) и трубопроводный (б)

Для установки технических средств обработки информации ограниченного доступа кроме специальных экранированных сооружений могут использоваться экранированные камеры, предназначенные для испытания технических средств по параметрам электромагнитной совместимости и обеспечивающие эффективность экранирования в полосе частот 0,01-37500 МГц.

В зависимости от эффективности экранирования и конструктивного исполнения ЭК подразделяют на три класса в соответствии с табл. 2.3.

Таблица 2.3 - Классы экранированных камер

Классы экранированных камер	**I класс**	**II класс**	**III класс**
Эффективность экранирования, дБ	Свыше 80 до 120	Свыше 30 до 80	До 30 Включительно
Конструктивное исполнение	Неразборная	Неразборная, сборно-разборная	

Неразборные ЭК должны состоять из конструктивно унифицированных типовых элементов, которые собирают на месте установки. Они могут быть стационарными и мобильными.

Мобильные (перевозимые) ЭК полностью собираются в заводских условиях и выполняются как перевозимые контейнеры на любом виде соответствующего транспорта.

Внешний вид мобильной экранированной камеры представлен на рис.2.8. Её габаритные размеры составляют: 12,0 (длина) х 4,5 (ширина) х 3,2 (высота) м, а вес 10 т.

ЭК укомплектована технологическим оборудованием, системами жизнеобеспечения и безопасности (принудительной приточно-вытяжной вентиляцией,

кондиционированием, автоматической системой газового пожаротушения и сигнализации) и предназначена для эксплуатации при температуре от -40 ^{0}C до +50 ^{0}C. Гарантийный срок службы этой ЭК составляет 10-15 лет.

Рисунок 2.8 - Мобильная (перевозимая) экранированная камера

Сборно-разборные ЭК должны состоять из конструктивно унифицированных типовых элементов, изготавливаемых в заводских условиях, которые собирают на месте установки.

Внешний вид сборно-разборной ЭК представлен на рис. 2.9.

Рисунок 2.9 - Сборно-разборное экранированное сооружение (камера):
а) вид снаружи; б) и в) вид внутри в экранированное сооружение для информационного обмена с установленной в нём аппаратурой.

Конструкция ЭК должна обеспечивать возможность многократной сборки-разборки камеры без снижения её эффективности экранирования.

Конструкция элементов ЭК должна иметь габариты, позволяющие транспортировать их через дверные проёмы помещений.

Панели и элементы ЭК соединяют между собой болтами и гайками с прокладкой уплотнителей.

Материалы и покрытия контактирующих элементов должны выбираться так, чтобы гальваноконтактное напряжение, возникающее между ними, не вызывало коррозийного напряжения.

Комплектацию ЭК типовыми элементами экранирования (дверьми, воротами, электрическими воздуховодными фильтрами, фильтрами для технологических вводов, светопроницаемыми проёмами), системой пожаротушения, сигнализацией, элементами освещения, телефонной связью проводят в соответствии с требованиями технического

задания на ЭК конкретного типа.

Конструкция ЭК должна быть электрогерметичной. Размеры ЭК выбирают с учётом целевого назначения, технологии проводимых работ, количества установленных технических средств, их габаритов, а также с учётом количества рабочих мест.

При размещении ЭК необходимо предусматривать проходы шириной не менее 1 м между стенками ЭК и выступающими конструкциями помещений для обеспечения сборки ЭК и проверки экрана.

Материал экрана должен обеспечивать:

- требуемую величину эффективности экранирования в заданном диапазоне частот;
- механическую прочность конструкции ЭК;
- технологичность изготовления и монтажа;
- устойчивость против коррозии.

Для ЭК I и II классов рекомендуется в качестве экрана применять листовую сталь следующих марок: холоднокатаная ст. 3 по ГОСТ 19904; горячекатаная ст. 3 по ГОСТ 19903; углеродная качественная и обыкновенного качества общего назначения ст. 3 по ГОСТ 16523.

В отдельных случаях может быть рекомендовано применение следующих металлических листовых материалов: листы из алюминия и алюминиевых сплавов по ГОСТ 21631; листы из алюминия и алюминиевых сплавов по ГОСТ 13726; листы и полосы медные по ГОСТ 495; ленты медные по ГОСТ 1173.

Для ЭК III класса рекомендуется в качестве экрана применять следующие материалы: фольгу алюминиевую для упаковки по ГОСТ 745; фольгоизол по ГОСТ 20429; фольгу медную электролитическую по ТУ 48-0318- 49; фольгу медную рулонную для технических целей по ГОСТ 5638; сетки стальные проволочные, тканевые с квадратными ячейками общего назначения по ГОСТ 3826; сетки латунные и бронзовые проволочные тканевые с квадратными ячейками нормальной точности по ГОСТ 6613.

Листы (панели) экрана, выполненные из стального проката и стальной сетки, соединяют герметичным, непрерывным швом, выполненным электродуговой сваркой в среде защитного газа по ГОСТ 14771.

Металлическую сетку из цветных металлов соединяют пайкой припоем ПОС-40 по ГОСТ 21931.

Конструкция экранированных дверей, ворот и щитов должна обеспечивать требуемую эффективность экранирования в заданном диапазоне частот.

В случае, когда конструкция дверей или ворот не обеспечивает требуемую эффективность экранирования, в ЭК предусматриваются экранированные многотамбурные системы.

Внутренние размеры тамбуров выбирают с учётом размеров дверей или ворот и возможности транспортировки ТСОИ и другого технического оборудования, необходимого для проведения работ внутри ЭК.

Конструкция экранированных дверей, ворот и щитов должна обеспечивать электрический контакт по периметру соприкосновения с полотном проёма коробки двери, ворот или щита.

Конструкция экранированных дверей должна быть распашного типа, не иметь механического запирающего устройства и открываться вручную изнутри и снаружи.

Конструкция экранированных ворот должна быть откатного варианта однопольного типа и должна предусматривать возможность их транспортировки от завода-изготовителя потребителю.

Система управления и сигнализация экранированных ворот должна предусматривать возможность отключения технических средств при нарушении их нормального функционирования.

Конструкция радиочастотных фильтров (РЧФ) для защиты вводов электрических

сетей, воздуховодов и трубопроводов должна обеспечивать требуемую эффективность экранирования в заданном диапазоне частот.

При невозможности обеспечения требуемой эффективности экранирования в заданном диапазоне частот одним типом фильтра допускается последовательное соединение требуемого числа фильтров одного или нескольких типов.

Конструкция радиочастотного фильтра для защиты вводов коммуникаций должна отвечать следующим требованиям:

- обладать достаточной механической прочностью, удобством крепления и монтажа;
- не содержать дефицитных и дорогостоящих деталей;
- иметь минимальные габаритные размеры и вес.

Места соединения корпуса радиочастотного фильтра с экраном ЭК должны иметь эффективность экранирования в заданном диапазоне частот не ниже эффективности экранирования ЭК. Способ соединения конструкции радиочастотных фильтров с экраном определяет разработчик ЭК.

РЧФ устанавливают в местах ввода в ЭК сетей освещения, силовых низковольтных и высоковольтных сетей, цепей управления, блокировки, сигнализации, связи и т. д.

Тип РЧФ выбирают с учётом: диапазона частот; величины требуемого вносимого затухания фильтра; количества вводимых проводов, вводов (жил кабеля); электрических параметров вводимых сетей (частоты и напряжения сети, силы тока постоянного и переменного); климатических и вибрационных условий; габаритных размеров, веса.

Корпуса РЧФ для защиты вводов электрических сетей должны иметь клемму заземления.

Радиочастотные воздуховодные фильтры (РЧВФ) устанавливают в местах ввода в ЭК систем вентиляции и кондиционирования воздуха.

Тип РЧВФ выбирают с учётом: диапазона частот; величины требуемой эффективности экранирования; размеров сечения вентиляционного проёма, выбираемого с учётом обеспечения требуемого воздухообмена и поддержания нормальных климатических условий в ЭК для работы обслуживающего персонала, ТС и обеспечения технологии проведения работ.

Радиочастотные трубопроводные фильтры (РЧТФ) устанавливают в местах ввода в ЭК трубопроводов отопления, водопровода.

Тип РЧТФ выбирают с учётом: диапазона рабочих частот; внутреннего геометрического размера трубопровода; радиотехнических характеристик среды, заполняющей полость трубопровода.

Экран камеры и металлические конструкции, связанные с установкой электрооборудования, которые могут оказаться под напряжением вследствие нарушения изоляции, должны быть заземлены в соответствии с требованиями ГОСТ 12.1.030 и СНиП 3.05.06.

Экран камеры должен быть связан с шиной заземления.

Жилы заземления и ответвления от них должны быть доступны для осмотра, кроме нулевых жил и заземляющих защитных проводников, проложенных в трубах и коробах.

Контактные соединения в цепи заземления или зануления должны соответствовать классу 2 по ГОСТ 10434.

Присоединение заземляющих и нулевых защитных проводников к частям оборудования, подлежащих заземлению или зану-лению, должно быть выполнено сваркой или болтовым соединением. Для болтового соединения должны быть предусмотрены меры против ослабления и коррозии контактного соединения.

Каждая часть технического средства, подлежащая заземлению или занулению, должна быть присоединена к сети заземления или зануления при помощи отдельного ответвления. Последовательное включение в заземляющий или нулевой защитный проводник заземляемых или зануляемых частей электроустановки не допускается.

ЭК не должны примыкать к стенам здания из лёгких ограждающих конструкций со сгораемыми и трудносгораемыми утеплителями.

Для изготовления ЭК должны применяться только несгораемые и трудносгораемые отделочные материалы.

Двери ЭК должны открываться по ходу эвакуации.

В ЭК площадью более 100 $м^2$ должны быть предусмотрены не менее двух выходов, расположенных рассредоточено.

Автоматика системы пожаротушения ЭК должна функционировать от датчиков, реагирующих на дым и тепло. Срабатывание этих датчиков должно обеспечивать отключение всех систем вентиляции ЭК и электропитания технических средств и другого оборудования.

Установка технических средств обработки информации ограниченного доступа в экранированных сооружениях и камерах с эффективностью экранирования свыше 60 дБ исключает возможность перехвата защищаемой информации не только по техническим каналам утечки информации, возникающим вследствие побочных электромагнитных излучений и их наводок, но и по каналам утечки, создаваемым методом «высокочастоного облучения» и внедрением в технические средства электронных устройств перехвата информации.

3. Заземление технических средств.

Одним из наиболее опасных технических каналов утечки информации на объектах информатизации является канал утечки информации, возникающий вследствие побочных электромагнитных излучений (ПЭМИ) технических средств обработки информации (ТСОИ). Такой канал утечки информации часто называют электромагнитным.

Эффективным способом снижения уровня ПЭМИ является экранирование их источников. При реализации электромагнитного экранирования необходимо заземление экрана источника ПЭМИ, под которым понимается преднамеренное электрическое соединение экрана с заземляющим устройством.

Заземляющее устройство включает заземлитель и заземляющие проводники, соединяющие экран с заземлителем.

Заземлитель - проводящая часть (заземляющий электрод) или совокупность соединённых между собой проводящих частей, находящихся в электрическом контакте с землёй непосредственно или через промежуточную проводящую среду.

Часть земли, находящаяся вне зоны влияния какого-либо заземлителя, электрический потенциал которой принимается равным нулю, называется зоной нулевого потенциала (относительная земля), а зона земли между заземлителем и зоной нулевого потенциала - зоной растекания (локальная земля). Поэтому под термином «земля» наиболее часто понимается земля в зоне растекания.

Заземление делится на два основных вида по выполняемой роли - рабочее (функциональное) и защитное.

Защитное заземление - заземление, выполняемое в целях электробезопасности, а рабочее заземление - заземление точки или точек токоведущих частей оборудования, выполняемое для обеспечения его работы (не в целях электробезопасности).

Заземление, используемое в целях электромагнитного экранирования, относится к рабочему заземлению, но оно выполняет также функции и защитного заземления.

В большинстве случаев все ТСОИ, установленные на объекте информатизации, заземляются на один общий заземлитель (одноточечная схема заземления). Шина, являющаяся частью заземляющего устройства и предназначенная для присоединения нескольких проводников с целью заземления, называется главной заземляющей шиной.

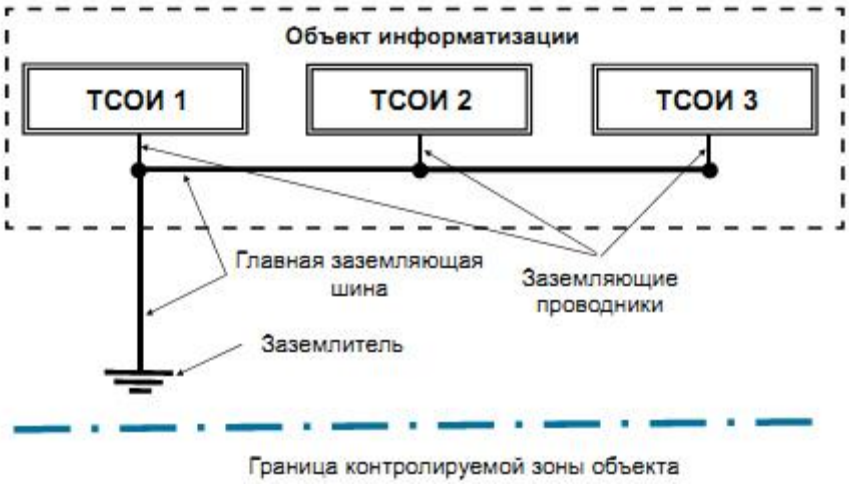


Рисунок 2.9 - Одноточечная последовательная схема заземления

В зависимости от способа подключения заземляющих проводников к заземлителю одноточечные схемы заземления подразделяются на последовательные, параллельные и комбинированные.

Одноточечная последовательная схема заземления наиболее проста (рис. 2.9). Однако ей присущи недостатки, связанные с протеканием обратных токов различных цепей по общему участку заземляющей цепи. Вследствие этого возможно появление опасного сигнала в посторонних цепях.

В одноточечной параллельной схеме заземления (рис. 2.10) этих недостатков нет. Однако такая схема требует большого числа протяжённых заземляющих проводников, из-за чего может возникнуть проблема с обеспечением малого сопротивления заземления участков цепи. Кроме того, между заземляющими проводниками могут возникать нежелательные связи, которые создают несколько путей заземления для каждого устройства. В результате в системе заземления могут возникнуть уравнительные токи и появиться разность потенциалов между различными устройствами.

При использовании одноточечной комбинированной (гибридной) схемы заземления ряд ТСОИ подключается к заземлителю последовательно, а ряд - параллельно (рис. 2.11).

Такая схема заземления наиболее часто используется на распределённых объектах информатизации: шина заземления прокладывается совместно по одной трассе с линиями электроснабжения. На участке от вводно-распределительного устройства или главного распределительного щита, где расположен главный заземляющий зажим, до щитков на этажах здания схема является параллельной одноточечной (одноточечной «звездой»), а на участке групповых сетей, от щитка до электрической розетки, - последовательной одноточечной.

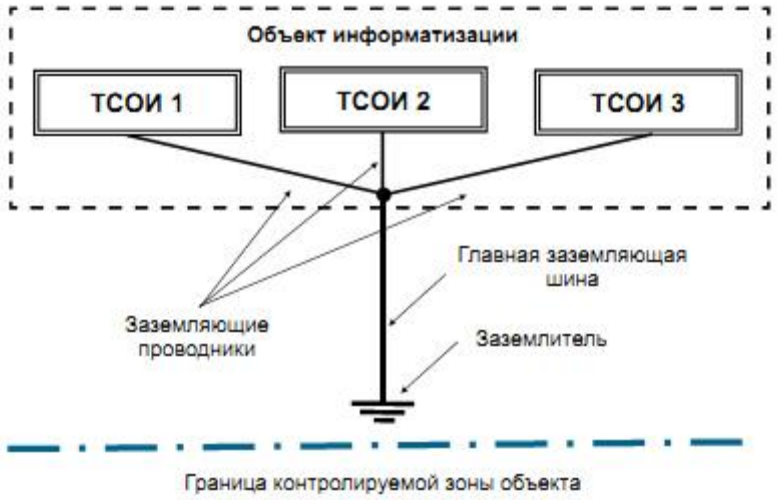


Рисунок 2.10 - Одноточечная параллельная схема заземления

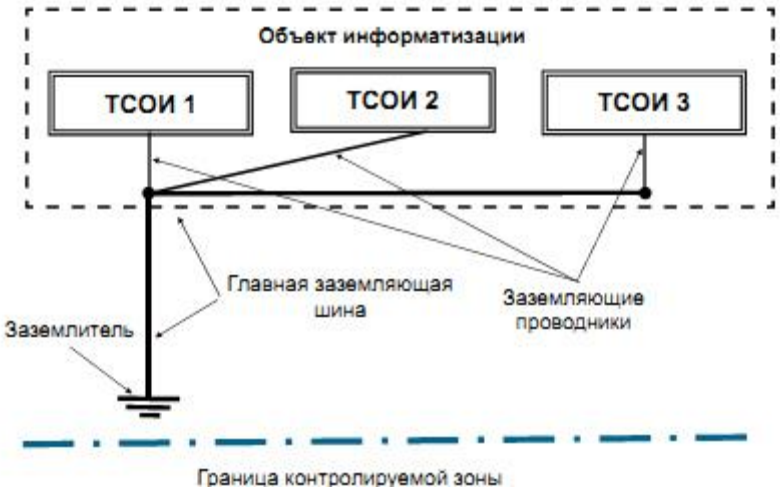


Рисунок 2.11 - Одноточечная комбинированная схема заземления

Заземление экранов ТСОИ должно быть выполнено в соответствии с определёнными правилами. Основные требования, предъявляемые к системе рабочего заземления объекта информатизации, заключаются в следующем:

1. система заземления должна включать заземлитель, шину заземления и заземляющие проводники, соединяющие за-землитель с экранами ТСОИ и их информативных кабелей;
2. запрещается использовать в качестве заземляющего устройства провода электросетей (нулевые фазы), металлоконструкции зданий, металлические оболочки подземных кабелей, металлические трубы систем отопления, водоснабжения, канализации;
3. главная заземляющая шина должна проходить как можно ближе к ТСОИ и быть соединена с его экраном заземляющим проводником наименьшей длины;
4. во избежание несанкционированного доступа к системе рабочего заземления все её элементы должны находиться в пределах контролируемой зоны объекта, при этом заземлитель не должен находиться ближе 10 м от её границы. В случае если это требование не выполняется, должно осуществляться линейное электромагнитное зашумление цепей заземления ТСОИ;
5. общее сопротивление заземлителя, заземляющих проводников и шин заземления не должно превышать 4 Ом;
6. каждый заземляемый элемент должен быть присоединён к заземлителю или к шине заземления при помощи отдельного проводника (рис. 2.12). Последовательное

включение в заземляющий проводник заземляемых технических средств не допускается (рис. 2.13);

7. следует избегать использования общих проводников в системе рабочего заземления, защитных заземлений и сигнальных цепей;

8. в системе заземления должны отсутствовать замкнутые контуры, образованные соединениями или нежелательными связями между сигнальными цепями и корпусами устройств, между корпусами устройств и землёй;

9. заземляющие проводники должны иметь покрытие, предохраняющее их от коррозии;

10. качество электрических соединений в системе заземления должно обеспечивать минимальное сопротивление контакта, надёжность и механическую прочность контакта в условиях климатических воздействий и вибрации;

11. присоединение шины заземления к за-землителю, а также заземляющих проводников к шине заземления должно быть выполнено сваркой или специальными зажимами, а заземляющих проводников к корпусам технических средств - болтовым соединением;

12. контактные соединения должны исключать возможность образования гальванических пар для предотвращения коррозии в цепях заземления. На контур рабочего заземления должны быть заземлены не только технические средства обработки иформации ограниченного доступа, но и вспомогательные технические средства и системы (ВТСС), а также посторонние проводники (металлические трубопроводы водопровода и центрального отопления, металлические конструкции внутри здания и т.д.).

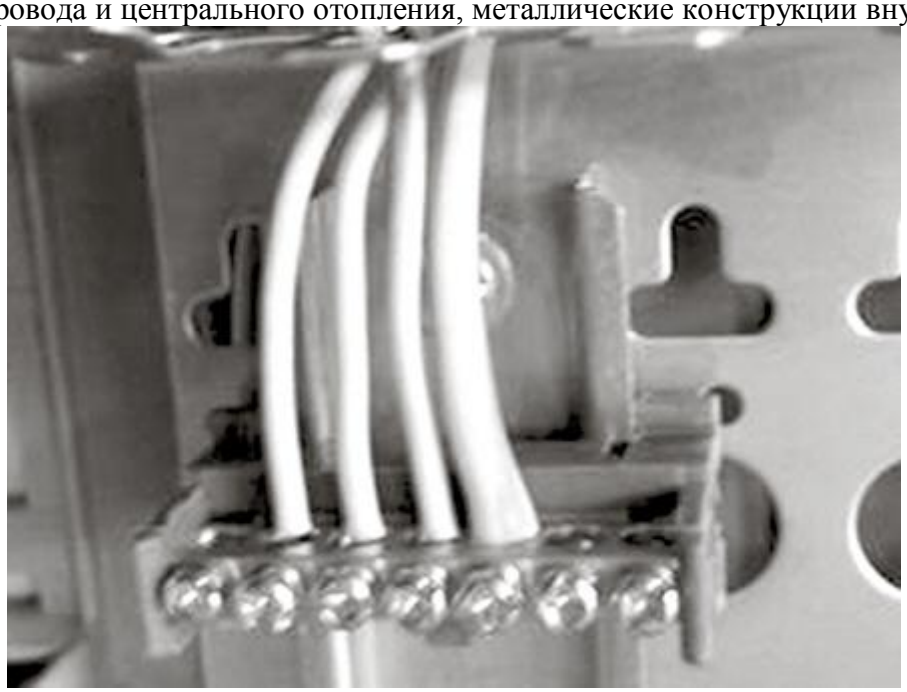


Рисунок 2.12 - Пример присоединения к главной шине заземления заземляющих проводников

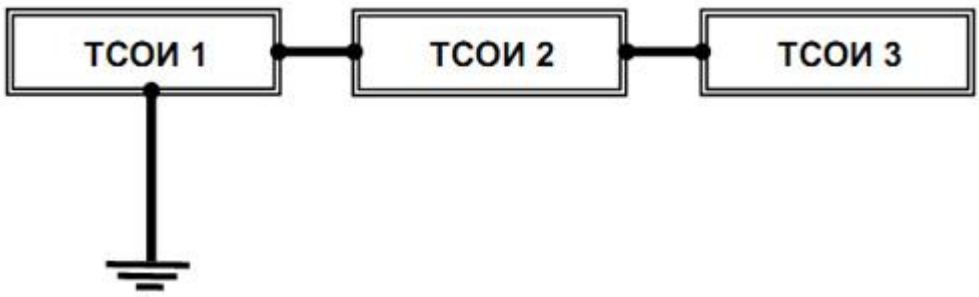


Рисунок 2.13 - Неправильно выполненая схема заземления

(последовательное включение в заземляющий проводник нескольких заземляемых устройств)

Неправильно выполненное заземление, например, наличие замкнутых контуров и связей между системами заземления различных технических средств обработки информации, может привести к существенному возрастанию уровня побочных электромагнитных излучений.

Такая ситуация может возникнуть, когда два технических средства обработки информации, заземлённых на рабочий контур заземления, соединены экранированным кабелем, соединяющим корпуса этих устройств (рис. 2.14). В данном случае по экрану кабеля и заземляющим проводникам начинает протекать некоторая доля наведённого в них информативного сигнала, образуя замкнутый контур, выполняющий функцию «случайной антенны». Совпадение резонансной частоты этой «случайной антенны» с одной из гармоник информативного сигнала может привести к существенному возрастанию уровня побочных электромагнитных излучений.

Поэтому экраны кабелей необходимо заземлять с одной стороны, например, со стороны основного оборудования.

С целью исключения «проникновения» наведённых высокочастотных информативных сигналов из заземляющих проводников рабочего заземления в систему защитного заземления следует применять: изолирующие трансформаторы; источники бесперебойного питания с двойным преобразованием частоты и изолирующим трансформатором; фильтры нижних частот (трансфильтры, суперфильтры) с изолирующим трансформатором. Основным условием применения этого обрудования является отсутствие кондуктивной связи с первичной стороной как по PE, так и по N проводникам.

Одним из основных требований, предъявляемых к рабочему заземлению, используемому в целях электромагнитного экранирования, является требование к сопротивлению заземления, которое не должно превышать 4 Ом.

Под сопротивлением заземления понимается отношение напряжения на заземляющем устройстве к току, стекающему с зазем-лителя в землю [6].

Сопротивление заземления определяется главным образом сопротивлением растекания тока в земле и зависит от площади электрического контакта заземлителя (заземляющих электродов) с грунтом и удельного электрического сопротивления грунта, в котором смонтирован этот заземлитель.

Удельное электрическое сопротивление грунта - параметр, определяющий уровень «электропроводности» грунта как проводника. Оно зависит от состава грунта, размеров и плотности прилегания друг к другу его частиц, влажности и температуры, концентрации в нём растворимых химических веществ (солей, кислотных и щелочных остатков), температуры и т.п. и колеблется в очень широких пределах (табл. 2.4).

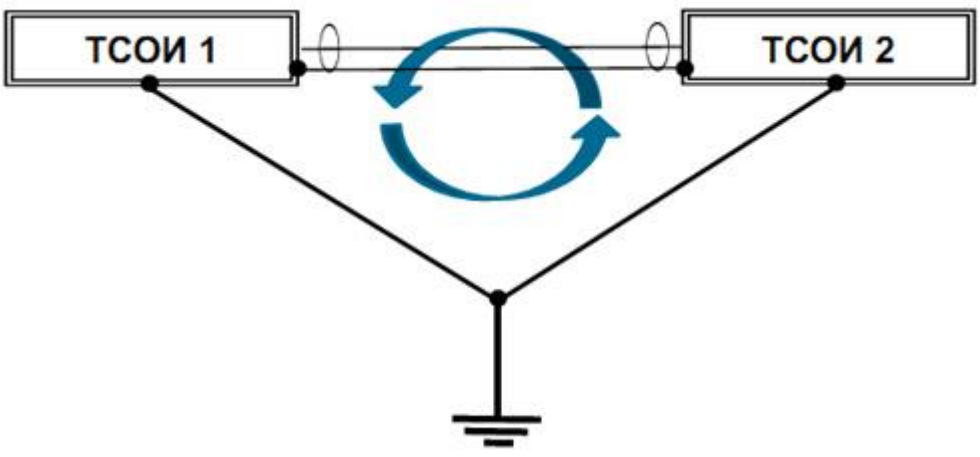


Рисунок 2.14 - Неправильно выполненная схема заземления (замкнутые контуры, образованные соединениями между корпусами устройств и землёй)

Величину сопротивления грунта можно значительно понизить за счёт уменьшения переходного сопротивления между заземли-телем и почвой путём тщательной очистки перед укладкой поверхности заземлителя и утрамбовкой вокруг него почвы, подсыпкой поваренной соли, а также орошением почвы вокруг заземлителей (орошение почвы вокруг заземлителей 2-5%-ным соляным раствором снижает сопротивление заземления в 5 - 10 раз).

Таблица 2.4 - Значения удельного сопротивления различных грунтов

Тип грунта	**Удельное сопротивление (ρ*), Ом/см^3**		
	среднее	**минимальное**	**максимальное**
Золы, шлаки, соляные отходы	2370	500	7000
Глина, суглинки, сланцы	4060	340	16300
Глина, суглинки, сланцы с примесями песка	15800	1020	135000
Гравий, песок, камни с небольшим количеством глины или суглинков	94000	59000	458000

Хорошо проводящие грунты теряют свои свойства при отсутствии влаги. Для большинства грунтов 30%-ного содержания влаги достаточно для обеспечения малого сопротивления. Например, для суглинков удельное сопротивление при влажности 5% составляет 165000 Ом/см^3, а при влажности 30% - 6400 Ом/см^3. Поэтому везде, где это возможно, заземлители следует помещать довольно глубоко - на уровне грунтовых вод либо на постоянном уровне влаги.

Изменение температуры почвы также значительно влияет на её удельное сопротивление (табл. 2.5).

При промерзании сопротивление грунтов резко возрастает. Например, для суглинков удельное сопротивление при влажности 15% и температуре 20^{o}C составляет 72 Ом/см^3, при температуре 5^{o}C - 790 Ом/см^3, а при температуре -15^{o}C - 3300 Ом/см^3.

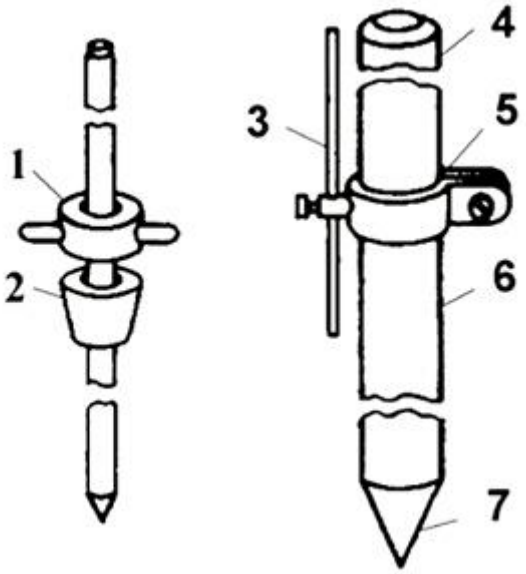
Таблица 2.5 - Влияние изменения температуры на удельное сопротивление почвы (для глинистого песка влажностью 15,2%)

Температура почвы, ^{o}C	**Удельное сопротивление почвы, Ом**
20	72
10	99
0 (вода)	138
0 (лед)	300
-5	790
- 15	3300

На практике наиболее часто в качестве заземлителей применяют:

- стержни из металла, обладающие высокой электропроводностью, погружённые в землю и соединённые с шиной заземления;

- сеточные заземлители, изготовленные из элементов с высокой электропроводностью и погружённые в землю (служат в качестве дополнения к заземляющим стержням).



Риунок 2.15 - Типовые стержни заземлителей:
1 - скользящий молот;
2 - подвижный упор;
3 - соединительная медная шина;
4 - головка с фаской;
5 - зажим;
6 - стержень;
7 - заострённый конец для забивки в грунт

В качестве одиночных стержневых за-землителей целесообразно использовать медные заземляющие стержни, конструкции которых приведены на рис. 2.15, или стальные трубы длиной 2-3 м и диаметром 35-50мм.

Учесть все факторы, влияющие на проводимость почвы, аналитическим путём практически невозможно, поэтому при устройстве заземления величину удельного сопротивления грунта в тех местах, где предполагается размещение заземления, определяют опытным путём.

На рис. 2.16 приведена схема комбинированного заземления из стержней и сетки.

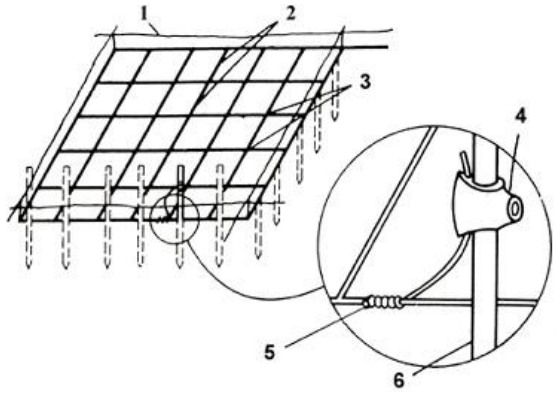


Рисунок 2.16 - Комбинированное заземление из стержней и сетки:
1 - поверхность земли; 2 - сетка; 3 - сварное соединение;
4 - зажим; 5 - медный провод (навитой и приваренный);
6 - медный стержень заземления (его верхний конец выступает над поверхностью)

При необходимости устройства рабочего заземления нужно учитывать не только геометрические размеры заземлителей, их конструкцию и свойства почвы, но и длину волны высокочастотного излучения. Суммарное высокочастотное сопротивление заземления Z_s складывается из высокочастотного сопротивления шины заземления Z_m (провода, идущего от заземляемого устройства до поверхности земли) и из высокочастотного сопротивления самого за-землителя$Z_з$ (провода, металлического стержня или листа, находящегося в земле).

На практике величина заземления экранов технических средств в основном определяется не сопротивлением заземлителя, а сопротивлением заземляющих проводников. Для уменьшения последнего следует стремиться прежде всего к уменьшению индуктивности заземляющих проводников, что достигается за счёт уменьшения их длины и изготовления шины заземления в виде ленты, обладающей по сравнению с проводом круглого сечения меньшей индуктивностью. В тех случаях, когда индуктивность заземляющей шины можно сделать весьма небольшой или использовать её для получения последовательного резонанса при блокировании излучающих сетей защитными конденсаторами на землю (например, при комплексном подавлении излучения в помещениях), целесообразно уменьшить величину сопротивления заземлителя $Z_з$

Уменьшить величину $Z_з$ можно путём применения многократного заземления, состоящего из ряда одиночных симметрично расположенных заземлителей, соединённых между собой. При этом общее сопротивление зазем-лителя будет тем меньше, чем дальше друг от друга расположены отдельные заземлители.

При использовании комбинированного заземлителя в качестве вертикальных электродов используют прутковую сталь диаметром не менее 10 мм или угловую сталь толщиной не менее 4 мм. Горизонтальные электроды используются для гальванического соединения между собой вертикальных электродов, а также самостоятельно. Для этих целей применяют полосовую сталь сечением не менее 48 мм^2 и сталь круглого сечения диаметром не менее 6 мм.

Для установки вертикальных заземлителей роют траншею. Верхние концы погружённых в землю вертикальных электродов соединяют стальной полосой с помощью сварки. В таких же траншеях прокладывают и горизонтальные электроды.

Проводник, соединяющий заземлитель с контуром заземления, должен быть лужёным для уменьшения гальванической коррозии, а соединения должны быть защищены от воздействия влаги.

Шины заземления вне здания необходимо прокладывать на глубине около 1,5 м, а внутри здания - по стене или специальным каналам таким образом, чтобы их можно было внешне осматривать. Шину заземления с заземлителем, как правило, соединяют с помощью сварки в одной точке, а заземляющие проводники подключают к ней с помощью болтового соединения.

Для уменьшения сопротивлений контактов наилучшим является постоянное непосредственное соединение металла с металлом, полученное сваркой или пайкой. При соединении под винт необходимо применять шайбы (звездочки или Гровера), обеспечивающие постоянство плотности соединения.

При соприкосновении двух металлов в присутствии влаги возникает гальваническая и/или электрическая коррозия. Гальваническая коррозия является следствием образования гальванического элемента, в котором влага служит электролитом. Степень коррозии определяется положением этих металлов в электрическом ряду. Электрическая коррозия может возникнуть при соприкосновении в электролите двух одинаковых металлов. Она определяется наличием локальных электротоков в металле, например, токов в заземлениях силовых цепей.

Наиболее эффективным методом защиты от коррозии является применение металлов с малой электрохимической активностью, таких, как олово, свинец, медь.

Значительно уменьшить коррозию и обеспечить хороший контакт можно, тщательно изолируя соединения от проникновения влаги.

В городских условиях часто существенно ограничена доступная для монтажа зазем-лителя площадь поверхности. В этих условиях используется модульная штыревая система заземления (МШСЗ), которая позволяет осуществить монтаж контура заземления любой конфигурации без применения сварки.

Вертикальные элементы заземлителей монтируются из стержней длиной 1,2-3 м и диаметром 14,2-17,2 мм. Снаружи каждый стальной стержень по всей длине покрывается методом электрохимического нанесения слоем меди толщиной не менее 250 мкм. Медное покрытие позволяет максимально снизить возможность ржавления металла и продляет срок годности изделий.

Стальной остроконечный наконечник навинчивается на стержень, вертикально вбиваемый в землю. Для различных типов грунта в зависимости от его твёрдости используются различные типы наконечников. Длина наконечников составляет 40-50 мм.

Для соединения стержней между собой применяются муфты, выполненные из латуни. Наращивание заземлителя производится путём присоединения к муфте следующего стержня.

С целью получения постоянной электрической цепи заземляющего вертикального электрода при монтаже на резьбовые соединения наносят всесезонную электропроводящую графитовую смазку. Она защищает от коррозии, и её применение уменьшает на 9-11% сопротивление стыка.

Для защиты мест соединения стержней от коррозии используют влагонепроницаемую антикоррозионную полимерно-асмольную или бутиловую клейкую ленту. Она обладает стойкостью к кислотам, щелочам, солям и микроорганизмам, не пропускает воду, водяной пар и газы.

При глубинном монтаже сопротивление заземлителей практически не зависит от времени года и погоды, что является несомненным преимуществом глубинного монтажа по сравнению с обычным.

Контур заземления, выполненный с помощью модульной штыревой системы, может иметь конфигурацию одноточечного или многоточечного.

Использование глубинного заземления позволяет значительно сократить не только площадь контура заземления, но и количество используемых стержней.

В городских условиях наиболее распространённая система распределения электроэнергии включает в себя электроустановку здания, которая подключена к низковольтной распределительной электрической сети.

Распределительная электрическая сеть, представляющая собой низковольтную электрическую сеть, к которой подключают электроустановки зданий, обычно состоит из понижающей трансформаторной подстанции напряжением 10/0,4 кВ и трёхфазной воздушной или кабельной линии электропередачи, имеющей четыре проводника: три фазных проводника (LI, L2, L3) и совмещённый защитный заземляющий и нейтральный проводник (PEN).

Все заземляющие проводники должны прокладываться изолированными проводами и кабелями. В электрических щитах шины и клеммники РЕ для ТСОИ должны размещаться изолированно от корпусов. Линии РЕ для заземления корпусов ТСОИ должны прокладываться отдельными проводами и кабелями от одного и того же главного заземляющего зажима.

На объектах информатизации наиболее часто в качестве технических средств обработки информации ограниченного доступа используются средства вычислительной техники (СВТ), в которых не предусмотрено болтового соединения заземляющих проводников. Заземление таких средств выполняется через контактные разъёмные соединения электрической розетки 220 В и питающего трехпроводного кабеля. Розетка должна обеспечивать надёжное соединение заземляющих проводников с экраном ТСОИ.

В настоящее время в России широко используются розетки европейского типа (так называемые «евророзетки»). У таких розеток заземляющий контакт имеет форму двух ламе-лей, расположенных на окружности розетки . Диаметр гнезда штепсельного разъёма у «евророзетки» составляет 4,8 мм.

При сдаче в эксплуатацию рабочего заземления объекта информатизации монтажной организацией должна быть представлена следующая документация:

- утверждённая проектная документация;
- план подземных электротехнических коммуникаций;
- исполнительные рабочие схемы электрических соединений;
- акты приёмки скрытых работ;
- технический паспорт заземляющего устройства;
- протоколы приёмо-сдаточных испытаний.

В техническом паспорте заземляющего устройства (ЗУ) рабочего заземления должны быть отражены:

- дата ввода ЗУ в эксплуатацию (дата реконструкции или ремонта ЗУ);
- основные параметры заземлителя (тип, материал, профиль, сечение проводников, их количество, глубина залегания и т.п.);
- удельное сопротивление грунта;
- результаты проверки ЗУ (дата проверки, сопротивление растеканию тока, сопротивление растеканию тока без отходящих коммуникаций, степень коррозии заземлителя, заключение о пригодности ЗУ к эксплуатации);
- результаты проверки связей оборудования объекта с заземлителем (дата проверки, наличие связи оборудования с ЗУ, сопротивление связи между оборудованием по заземлителю, заключение о пригодности заземлителя оборудования к эксплуатации);
- сведения об изменениях после ремонта или реконструкции ЗУ (перечень изменений, вид работ (замена оборудования, ремонт, реконструкция), время проведения работ, организация-исполнитель, отметка о внесении изменений в план-схему ЗУ);
- ведомость дефектов (дата проверки, оборудование, обнаруженные дефекты, устранение дефектов (организация-исполнитель, отметка об устранении дефектов, дата).

К паспорту должна прилагаться план-схема ЗУ (выполненная в масштабе) с указанием мест установки заземлителей, прокладки шин заземления и заземляющих проводников, мест и способа крепления проводников к заземлителю и шине заземления и т.п.

2.8 Лабораторная работа № 8 (2 часа).

Тема: «Методы и средства выявления электронных устройств негласного получения информации**»**

2.8.1 Цель работы: изучить методы и средства выявления электронных устройств негласного получения информации

2.8.2 Задачи работы:

1. Методы выявления электронных устройств негласного получения информации, внедренных в выделенные помещения и технические средства.
2. Средства выявления электронных устройств негласного получения информации: индикаторы электромагнитного поля, программно-аппаратные комплексы радиоконтроля, анализаторы проводных коммуникаций, нелинейные локаторы, рентгено-телевизионные комплексы.
3. Порядок проверки технических средств и выделенных помещений на наличие электронных устройств негласного получения информации.

2.8.3 Перечень приборов, материалов, используемых в лабораторной работе:

1. Персональный компьютер, специальное ПО

2.8.4 Описание (ход) работы:

1. Методы выявления электронных устройств негласного получения информации, внедренных в выделенные помещения и технические средства.

Электронными устройствами перехвата информации называются скрытно внедряемые в места возможного съема информации малогабаритные электронные устройства, предназначенные для несанкционированного съема информации. Такие устройства часто называют закладными (закладочными) устройствами (ЗУ), или просто закладками.

В зависимости от вида информации, перехватываемой закладными устройствами, последние можно разделить на акустические, телефонные и аппаратные закладки, а также закладные телевизионные системы.

Акустические закладки предназначены для перехвата акустической (речевой) информации.

Перехватываемая акустическими закладками информация может записываться с использованием портативных устройств звукозаписи (цифровых диктофонов) или передаваться по радиоканалу, оптическому каналу, электросети переменного тока, телефонной линии, соединительным линиям вспомогательных технических средств (ВТСС), трубам систем отопления и водоснабжения, по специально проложенным линиям и т.д.

Акустические закладки могут быть построены по принципу классического передающего устройства, включающего как задающий генератор, так и модулятор. А могут быть построены по схеме полуактивного устройства типа аудиотранспондера или эндовибратора, в которых роль сигнала задающего генератора выполняет внешнее излучение.

Современные ЗУ способны не только перехватывать разговоры, ведущиеся в помещениях, но и осуществлять видеозапись. Видеоизображения с телевизионных камер могут записываться на цифровые накопители или передаваться по радиоканалу с использованием специальных видеопередатчиков. Одновременно возможна запись или передача не только изображений, но и звука.

Для передачи информации используются в основном диа-пазоны частот VHF, UHF и SHF. Наиболее часто используется диапазон 2,4 ГГц.

Акустические закладки и телевизионные ЗУ в обычном исполнении (в виде отдельных модулей) могут скрытно устанавливаться (внедряться) в ограждающие конструкции (например, стены помещения) и предметы интерьера помещений (письменный стол, книжный шкаф и т.п.), технические средства и системы обработки информации (ПЭВМ), электроприборы (настольную электрическую лампочку), радиоприборы (телевизор), вспомогательные технические средства и системы (датчики охранной и пожарной сигнализации) и т.д.

Камуфлированные закладки, как правило, встраиваются в небольшие по размеру предметы повседневного обихода: вазу, скоросши-ватель, настольные или настенные часы, пепельницу, электронный калькулятор, зажигалку, авто-ручку, электрическую розетку и т.п. Причем визуально отличить обычный предмет от камуфлированного под него ЗУ практически невозможно.

Телефонными закладками называются закладки, предназначенные для перехвата информации, передаваемой по телефонным линиям связи. Перехваченная информация может записываться на цифровые диктофоны или передаваться по радиоканалу.

Телефонные закладки используют те же виды сигналов, способы накопления информации и способы кодирования информации, что и акустические закладки.

Под аппаратной закладкой обычно понимают электронное устройство, скрытно устанавливаемо (внедряемое) в техническое средство обработки и передачи информации (ТСОИ) с целью обеспечить в нужный момент времени утечку информации, нарушение ее целостности или блокирование.

Наиболее часто используются аппаратные закладки, устанавливаемые в автоматизированные системы (АС), построенные на основе средств вычислительной техники (СВТ). По виду перехватываемой информации аппаратные закладки можно разделить на следующие:

- для перехвата изображений, выводимых на экран монитора;
- для перехвата информации, вводимой с клавиатуры ПЭВМ;
- для перехвата информации, выводимой на периферийные устройства (например, принтер);
- для перехвата информации, записываемой на жесткий диск ПЭВМ (HDD);
- для перехвата информации, записываемой на внешние накопители (flash-память, CD, DVD, USB-накопители и т.п.).

Аппаратная закладка, как правило, состоит из: блока перехвата, блока передачи информации (или модуля записи информации), блока дистанционного управления (при необходимости) и блока питания.

Блок перехвата подключается к информационным кабелям или непосредственно к платам блоков СВТ и осуществляет перехват информационных сигналов, их обработку и преобразование в вид, удобный для записи или передачи на приемный пункт. Перехватываемая аппаратными закладками информация может записываться в память ЗУ (например, на flash-память) или передаваться на прием-ный пункт по радиоканалу, электросети 220 В, оптическому каналу (при использовании ИК-порта), выделенной линии и т.п. С использованием системы дистанционно-го управления осуществляется включение/выключение устройства (запуск программы перехвата информации), включение/выключение режима передачи информации, установка параметров процесса съема и передачи информации.

Демаскирующие признаки электронных устройств перехвата информации.

Обнаружение ЗУ производится по их демаскирующим признакам. Под демаскирующими будем понимать признаки, по которым эти устройства можно обнаружить визуально или с использованием технических средств. Каждый вид электронных устройств перехвата информации имеет свои специфические демаскирующие признаки. Рассмотрим основные из них.

Демаскирующими признаками проводной микрофонной системы являются:

- скрытно проложенная линия (провод) неизвестного назначения, входящая в выделенное помещение и, как правило, выходящая за пределы контролируемой зоны;
- наличие в линии (проводе) неизвестного назначения постоянного напряжения (3 - 15 В) и низкочастотного информационного сигнала (при осуществлении пере-хвата информации);
- наличие на конце линии (провода) малогабаритно-го микрофона (часто закамуфлированного), скрытно установленного в выделенном помещении.

Демаскирующие признаки автономных некамуфлированных акустических закладок включают:

- признаки внешнего вида - малогабаритный предмет (часто в форме параллелепипеда) неизвестного назначения;
- одно или несколько отверстий малого диаметра в корпусе;
- небольшой отрезок провода (антенна), выходящий из корпуса закладки (как правило);
- наличие автономных источников питания (например, аккумуляторных батарей);
- наличие полупроводниковых элементов, выявляемых при облучении обследуемого устройства нелинейным радиолокатором;
- наличие в устройстве проводников и радиоэлектронных деталей, выявляемых при использовании рентгеновской техники.

Камуфлированные акустические закладки по внешнему виду на первый взгляд не отличаются от объекта имитации, особенно если закладка устанавливается в корпус бытового предмета без изменения его внешнего вида. Такие закладки можно выявить путем разборки предмета. Закладки, устанавливаемые в малогабаритные предметы,

ограничивают возможности последних. Эти ограничения могут служить косвенными признаками наличия ЗУ. Чтобы исключить возможность выявления закладки путем ее разборки, места соединения разбираемых частей склеивают. Некоторые камуфлированные ЗУ не отличаются от оригиналов даже при тщательном внешнем осмотре. Их можно обнаружить только при использовании рентгеновской техники.

В раде случаев закамуфлированное ЗУ обнаруживается по наличию в обследуемом предмете не свойственных ему радиоэлектронных элементов, выявляемых при облучении его нелинейным радиолокатором или при использовании рентгеновской техники. Например, обнаружение полупроводниковых элементов в пепельнице или в папке для бумаг может указать на наличие в них ЗУ.

Демаскирующие признаки акустических радиозакладок:

- радиоизлучение, источник которого находится в выделенном помещении;
- особенности излучений передатчиков ЗУ в ближней зоне (высокий уровень сигнала относительно сигналов других радиоэлектронных средств, наличие излучений на гармониках и субгармониках основной частоты излучения, значительное изменение уровня сигнала в пределах выделенного помещения, значительное уменьшение уровня сигнала за пределами выделенного помещения т.п.);
- корреляция изменения спектра радиосигнала с изменением параметров тестового акустического сигнала в выделенном помещении (при использовании для передачи информации аналоговых сигналов с простыми видами модуляции);
- характерные особенности радиосигналов с дельтамодуляцией (при использовании для передачи цифровых сигналов) и т.п.

Демаскирующие признаки полуактивных акустических радиозакладок:

- облучение помещения направленным (зондирующим) мощным гармоническим излучением;
- наличие в выделенном помещении источника вторичного излучения;
- корреляция изменения спектра вторичного излучения (переизлученного сигнала) с изменением параметров тестового акустического сигнала в выделенном помещении;
- амплитудная или частотная модуляция информационным акустическим сигналом.

Демаскирующие признаки акустических закладок типа «телефонного уха»:

- отличие параметров контролируемой телефонной линии (емкости, индуктивности, сопротивления и т.п.) при положенной и снятой телефонной трубке контролируемого аппарата от типовых значений;
- наличие тока утечки (от единиц до нескольких десятков мА) в телефонной линии при отключенном телефоне;
- подавление одногодвух сигналов вызова при наборе номера контролируемого телефонного аппарата;
- наличие в телефонной линии низкочастотного сигнала при положенной трубке телефонного аппарата;
- невозможность дозвона по телефонному номеру в течение длительного времени и т.д.

Демаскирующие признаки акустических сетевых закладок:

- наличие в линии электропитания (розеточной или осветительной сети выделенного помещения) информативного высокочастотного сигнала, источник которого находится в выделенном помещении;
- корреляция изменения спектра сигнала с изменением параметров тестового акустического сигнала в выделенном помещении (при использовании для передачи информации аналоговых сигналов с простыми видами модуляции);
- характерные особенности сигналов с дельта-модуляцией (при использовании для передачи цифровых сигналов);
- значительное превышение уровня сигнала в контролируемой линии над уровнем сигнала в линии электропитания, подключенной к другой фазе;
- наличие тока утечки (от единиц до нескольких десятков мА) в линии электропитания при всех отключен-ных потребителях;

• отличие параметров линии электропитания (емкости, индуктивности, сопротивления и т.п.) от типовых значений при отключении линии от источника питания (на распределительном щитке) и отключении всех потребителей.

Наличие звукозаписывающих и видеозаписывающих устройств в момент записи можно обнаружить по наличию их побочных электромагнитных излучений (излучений генераторов подмагничивания, электродвигателей, аналогово-цифровых преобразователей).

Телевизионные ЗУ, как правило, имеют объективы типа pin-hole, которые можно обнаружить по характерному отражению оптического излучения в видимом и ближнем ИК-диапазонах длин волн. Спектр телевизионного сигнала имеет ряд характерных особенностей, поэтому телевизионные передатчики легко обнаружить по их радиоизлучениям.

Демаскирующие признаки акустических закладок с передачей информации по телефонной линии на высокой частоте аналогичны рассмотренным выше.

Демаскирующие признаки телефонных радиозакладок:

• радиоизлучение, возникающее при снятии трубки контролируемого телефонного аппарата;
• корреляция изменения спектра радиосигнала с изменением параметров телефонного сигнала (при использовании для передачи информации аналоговых сигналов с простыми видами модуляции);
• характерные особенности сигналов с дельта-модуляцией (при использовании для передачи цифровых сигналов);
• отличие параметров контролируемой телефонной линии (емкости, индуктивности, сопротивления и т.п.) при положенной и снятой телефонной трубке контролируемого аппарата от типовых значений;
• падение напряжения (от нескольких десятых до 1,5 - 2 В) в телефонной линии (по отношению к другим телефонным линиям, подключенным к данной распределительной коробке) при положенной и поднятой телефонной трубке;
• наличие тока утечки (от единиц до нескольких десят-ков мА) в телефонной линии при отключенном телефоне.

К основным **демаскирующим признакам аппаратных закладок**, внедренных в технические средства обработки информации, относятся:

• признаки внешнего вида - наличие блоков или устройств неизвестного назначения, подключенных к информационным кабелям или платам блоков СВТ; наличие дополнительных плат, изменение в штатных печатных платах или появление в блоках дополнительных радиоэлементов; наличие на платах мест со следами свежей пайки; отличие элементов (микросхем, транзисторов, конденсаторов, резисторов и т.п.) от заводских (по внешнему виду, размерам, отсутствию соответствующих надписей и т.п.);
• радиоизлучение сравнительно большой мощности, источник которого находится в контролируемом техническом средстве;
• корреляция изменения спектра радиосигнала с изменением режимов работы технического средства;
• оптическое излучение ИК-порта при его отключении программным способом;
• отличие рентгеновских снимков (изображений) блоков или печатных плат контролируемого средства от типовых - наличие дополнительных элементов (микросхем, транзисторов, диодов, резисторов, конденсаторов и т.п.), несоответствие их расположения типовому, наличие дополнительных соединений, проводников и т.д.

Классификация методов и средств поиска (выявления) электронных устройств перехвата информации

Выявление внедренных в помещения и технические средства электронных ЗУ осуществляется в процессе специальных обследований и специальных технических проверок объектов информатизации и выделенных помещений.

Специальное обследование объектов информатизации и выделенных помещений

проводится без применения технических средств. В ходе специального обследования поиск ЗУ осуществляется по демаскирующим признакам их внешнего вида путем визуального осмотра помещения: стен, потолков, полов, дверей, оконных рам, предметов интерьера и мебели. Особое внимание уделяется местам, куда можно быстро и скрытно установить ЗУ: под столешницами, сиденьями стульев, в различных щелях, за карти-нами, батареями, мебелью, шторами и т.д. Осмотру также подвергаются средства оргтехники, электрические приборы и радиоэлектронная аппаратура, средства и системы охранной и пожарной сигнализации, телефонные аппараты и т.д. При проведении специального обследования проводится тестовый «прозвон» телефонных аппаратов в целях обнаружения закладных устройств типа «телефонного уха».

Специальная техническая проверка объектов информатизации и выделенных помещений проводится с использованием специальных технических средств и аппаратуры: индикаторов (детекторов) электромагнитного поля, радиочастотомеров, сканирующих приемников, интерсепторов, анализаторов спектра, программно-аппаратных комплексов радиоконтроля, нелинейных локаторов, рентгеновских и рентгено-телевизионных комплексов, анализаторов проводных линий и т.д.

Эффективность поиска ЗУ во многом определяется использованием той или иной аппаратуры контроля. К основным методам поиска ЗУ с использованием технических средств относятся:

- проверка помещений с использованием индикаторов (детекторов) электромагнитного поля;
- проверка помещений с использованием оптических средств поиска скрытых видеокамер;
- радиоконтроль (радиомониторинг) помещений;
- измерение параметров проводных линий;
- нелинейная локация;
- рентгеноскопия.

Проверка помещений с использованием индикаторов (детекторов) электромагнитного поля (далее - индикаторов поля) проводится в целях выявления ЗУ (радиозакладок - аппаратных закладок, акустических радиозакладок, телевизионных передатчиков), внедренных в выделенные помещения и на объекты информатизации и использующих для передачи информации радиоканал, а также диктофонов и устройств скрытой видеозаписи.

Принцип действия индикаторов (детекторов) электромагнитного поля основан на интегральном методе измерения уровня электромагнитного поля в точке их расположения. При поиске ЗУ с использованием индикаторов поля используются амплитудный метод и метод «акустической завязки».

Для обнаружения радиозакладок используются индикаторы поля с электрическими антеннами, обеспечивающие прием и детектирование радиосигналов в диапазоне час-тот от 30 - 100 МГц до 3 - 6 ГГц и более. Такие индикаторы поля позволяют обнаружить ЗУ, использующие для передачи информации практически все виды радиосигналов, включая широкополосные шумоподобные и сигналы с псевдослучайной скачкообразной перестройкой несущей частоты.

Поиск радиозакладок с использованием индикаторов поля наиболее целесообразен и эффективен в местах с низким уровнем общего электромагнитного поля, то есть вдали от крупных городов, объектов с большой концентрацией мощных радиоэлектронных средств и т.п.

Для обнаружения диктофонов и устройств скрытой видео-записи используются индикаторы поля с магнитными антеннами, которые осуществляют прием и детектирование побочных электромагнитных излучений, создаваемых диктофоном или устройством скрытой видеозаписи (видео-камерой или цифровым накопителем) в режиме записи.

Поиск ЗУ с использованием индикаторов поля осуществляется путем последовательного осмотра помещения вдоль стен и в обход мебели, предметов

интерьера, технических средств. При этом расстояние от антенны до обследуемых объектов должно быть не более 10 - 30 см. Места значительного превышения уровня сигнала над фоновым осматриваются визуально.

Проверка помещений с использованием оптических средств поиска осуществляется в целях обнаружения скрытых видеокамер, имеющих объективы типа pin-hole.

Обнаружение скрытых видеокамер с использованием оптических средств обеспечивается за счет эффекта отражения объективом видеокамеры оптического излучения, формируемого специальным устройством, в направлении источника зондирующего излучения. Объективы видеокамер зеркально отражают оптическое излучение в направлении на зондирующий излучатель в сравнительно узком телесном угле. При этом яркость отраженного излучения от объектива, как правило, на несколько порядков выше яркости диффузных вторичных источников. Для облучения используется монохроматическое излучение в видимом или ближнем инфракрасном диапазоне длин волн. Обнаружение видеокамер происходит по оптическому признаку, что позволяет обнаруживать скрытые видеосистемы как в режиме записи, так и в выключенном состоянии. Обнаружение скрытых видеокамер осуществляется путем последовательного осмотра прибором стен, потолка, мебели и предметов интерьера из возможных мест нахождения персонала в помещении.

Радиоконтроль (радиомониторинг) проводится в целях выявления ЗУ, внедренных в выделенные помещения и на объекты информатизации и использующих для передачи информации радиоканал. Он осуществляется с использованием комплексов радиоконтроля (КРК), построенных на базе сканирующих приемников или анализаторов спектра, а также программно-аппаратных комплексов радиоконтроля (ПАКРК).

Комплексы радиоконтроля разворачиваются или непосредственно в контролируемом помещении, или в специальном помещении, или в автомашине, припаркованной вблизи объекта контроля. При этом выносные антенны комплексов устанавливаются в контролируемых помещениях.

Радиоконтроль основан на приеме и анализе радиосигналов ЗУ. В процессе выявления ЗУ с использованием КРК можно выделить три этапа:

• обнаружение сигналов;

• идентификация сигналов;

• определение местоположения ЗУ в помещении (этап локализации).

Возможности по выявлению ЗУ во многом определяются реализованными в КРК методами обнаружения, идентификации сигналов и локализации их источников. Этап обнаружения заключается в выявлении неизвестных радиосигналов на контролируемом объекте. Методы обнаружения: превышение уровня сигнала установленного порога; превышение уровня сигнала над «фоновым спектром». Этап идентификации сигнала заключается в определении местоположения его источника (находится ли источник сигнала внутри или вне контролируемого помещения).

К основным методам идентификации относятся:

- сравнение уровней сигналов от внешней (опорной) антенны, установленной вне контролируемого помещения, и внутренней антенны, установленной в контролируемом помещении, - метод разнесенных антенн (или метод опорной антенны);
- сравнение тестового акустического сигнала в контролируемом помещении с низкочастотным демодулированным сигналом - низкочастотный корреляционный метод (или акустический тест);
- сравнение спектров сигнала при наличии и отсутствии тестового акустического сигнала в контролируемом помещении - высокочастотный корреляционный метод (или параметрический тест);
- проверка на наличие гармоник основного сигнала - тест на гармоники;
- детальный анализ сигнала.

Определение местоположения ЗУ осуществляется в том случае, если установлено, что источник обнаруженного сигнала находится в контролируемом помещении. Локализация ЗУ может производиться автоматически методом акустолокации или оператором в ручном режиме амплитудным или пеленгационным методами. Радиоконтроль может вестись постоянно, а также проводиться периодически. Наиболее эффективным является постоянный (круглосуточный в течение длительного времени) радиоконтроль. В этом случае могут быть выявлены не только дистанционно управляемые радиозакладки, но и закладки с промежуточным накоплением информации и использующие для передачи информации аппаратуру быстродействия.

Для ведения постоянного радиоконтроля в специально оборудованном помещении на объекте разворачивается стационарный пункт радиоконтроля, в состав которого включаются один или несколько многоканальных ПАКРК, выносные антенны которых устанавливаются в контролируемых помещениях.

Периодический радиоконтроль проводится при аттестации объектов, а также в период проведения особо важных мероприятий (совещаний, переговоров, встреч и т.п.) В этом случае в одном из помещений объекта, находящемся вблизи контролируемых помещений, разворачивается пункт радиоконтроля, а в контролируемых помещениях устанавливаются выносные антенны. Пункт радиоконтроля также может быть развернут в автомашине, припаркованной вблизи объекта контроля.

Измерение параметров проводных линий проводится в целях выявления ЗУ, непосредственно (гальванически) подключаемых к ним, и позволяет выявить:

- телефонные закладки, подключаемые к телефонной линии как последовательно, так и параллельно (в том числе через конденсатор);
- акустические закладки, использующие телефонную линию для передачи информации на низкой или высокой частоте;
- сетевые закладки, использующие линии электросети для передачи информации на высокой частоте;
- акустические закладки, использующие телефонную линию в качестве источника питания;
- акустические закладки, использующие линию электросети в качестве источника питания;
- микрофонные системы, использующие слаботочные линии для передачи информации на низкой частоте.

Измерением параметров линии также можно обнаружить подключение к ней аппаратуры высокочастотного навязывания. Объем и виды проводимых измерений зависят от типа проверяемой линии (сети электропитания, абонентской телефонной сети, системы часофикации, систем пожарной и охранной сигнализаций и т.д.).

При контроле проводных линий могут проводиться измерения:

- напряжений сигналов высокой частоты в линии (сигналов «высокочастотного навязывания»);
- напряжений низкочастотного сигнала в линии;
- напряжений постоянного и переменного токов в линии;
- тока короткого замыкания и сопротивления шлейфа линии;
- токов утечки в линии;
- сопротивления линии;
- емкости линии;
- индуктивности линии;
- нагрузочной характеристики (зависимости напряжения линии от тока нагрузки);
- переходной характеристики (реакции проверяемой линии на воздействие высоковольтного скачкообразно нарастающего напряжения);
- вольтамперной характеристики (зависимости тока, протекающего в проверяемой линии, от воздействия линейно нарастающего напряжения);
- характеристики «Лиссажу» (параметрической зависимости тока, протекающего в проверяемой линии, при воздействии синусоидального напряжения) и т.п.

При обнаружении в линиях электросети 220 В или телефонных линиях напряжения сигнала высокой частоты с использованием анализатора спектра или сканирующего приемника производятся измерение частоты сигнала и определение вида его модуляции. При необходимости осуществляются демодуляция и прослушивание сигналов с частотной или амплитудной модуляцией с использованием головных телефонов. При обнаружении в линии цифровых сигналов проводится исследование их спектра. При идентификации обнаруженных сигналов используются методы, аналогичные используемым при обнаружении радиозакладок. Поиск ЗУ, подключенных к проводной линии, производится путем ее визуального осмотра по всей длине.

Метод нелинейной локации используется для выявления ЗУ, внедренных в выделенные помещения, а также определения мест их подключения к проводным линиям. Данный метод основан на способности радиоэлектронных элементов, имеющих в своем составе полупроводники, отражать сигнал на второй гармонике частоты зондирующего сигнала. Для поиска ЗУ, внедренных в выделенные помещения, используются нелинейные радиолокаторы, а для определения мест их подключения к проводным линиям - нелинейные локаторы проводных линий.

Нелинейные радиолокаторы способны обнаружить ЗУ, внедренные в стены, потолки, полы, двери, оконные рамы, предметы интерьера, мебель и т.п., независимо от того, находится ли это устройство во включенном или выключенном состоянии.

Процесс поиска ЗУ с использованием нелинейного радиолокатора включает два этапа:

• обнаружение электронного устройства;

• идентификацию обнаруженного устройства.

Обнаружение электронного устройства происходит при превышении уровня отраженного сигнала на второй гармонике установленного порога.

Для идентификации обнаруженного устройства используются следующие методы:

• сравнение уровней отраженных сигналов на второй и третьей гармониках;

• наблюдение изменения уровня отраженного сигнала при механическом воздействии на обнаруженное устройство;

• наблюдение изменения уровня отраженного сигнала при изменении частоты зондирующего сигнала;

• прослушивание демодулированного низкочастотного сигнала на частоте второй гармоники через головные телефоны при изменении местоположения антенны радиолокатора относительно обнаруженного устройства;

• прослушивание демодулированного низкочастотного сигнала на частоте второй гармоники через головные телефоны при механическом воздействии на обнаруженное устройство;

• прослушивание демодулированного низкочастотного сигнала на частоте второй гармоники через головные телефоны при изменении частоты зондирующего сигнала.

Нелинейные локаторы проводных линий предназначены для определения факта подключения к проводным линиям (как силовым, так и слаботочным) электронных устройств перехвата информации, а также расстояний до мест их подключения. Принцип действия таких приборов заключается в подаче в линию зондирующего сигнала и регистрации отраженных от подключенных к линии ЗУ высших гармоник тока, возникающих в полупроводниковых элементах этих устройств при воздействии зондирующего сигнала.

Метод рентгеноскопии используется для выявления ЗУ, внедренных в ограждающие конструкции помещений, предметы интерьера, мебель, технические средства, в том числе радиоэлектронную аппаратуру, когда визуально выявить ЗУ невозможно.

Данный метод заключается **в рентгеновским облучении** обследуемых объектов (предметов) и получении их изображений. Анализ полученных рентгеновских изображений позволяет выявить внутреннюю структуру обследуемых объектов и

предметов и, следовательно, обнаружить внедренные (встроенные) в них ЗУ. Съемка может производиться с использованием рентгеновской аппаратуры фотографического типа (изображения фиксируются на специальной пленке) или с использованием рентгено-телевизионных установок (изображения выводятся на телевизионные экраны).

2. Средства выявления электронных устройств негласного получения информации.

Поиск и обнаружение закладных устройств может осуществляться визуально, а также с использованием специальной аппаратуры: детекторов диктофонов и видеокамер, индикаторов поля, радиочастотомеров и интерсепторов, сканерных приемников и анализаторов спектра, программно-аппаратных комплексов контроля, нелинейных локаторов, рентгеновских комплексов, обычных тестеров, а также специальной аппаратуры для проверки проводных линий и т.д.

Метод поиска закладных устройств во многом определяется использованием той или иной аппаратуры контроля. К основным методам поиска закладных устройств можно отнести:

- специальное обследование выделенных помещений;
- поиск радиозакладок с использованием индикаторов поля, радиочастотомеров и интерсепторов;
- поиск радиозакладок с использованием сканерных приемников и анализаторов спектра;
- поиск радиозакладок с использованием программно-аппаратных комплексов контроля;
- поиск портативных звукозаписывающих устройств с использованием детекторов диктофонов (по наличию их побочных электромагнитных излучений генераторов подмагничивания и электродвигателей);
- поиск портативных видеозаписывающих устройств с использованием детекторов видеокамер (по наличию побочных электро-магнитных излучений генераторов подмагничивания и электродвигателей видеокамер);
- поиск закладок с использованием нелинейных локаторов;
- поиск закладок с использованием рентгеновских комплексов;
- роверка с использованием ВЧ-пробника (зонда) линий электропитания, радиотрансляции и телефонной связи;
- измерение параметров линий электропитания, телефонных линий связи и т.д.;
- проведение тестового "прозвона" всех телефонных аппаратов, установленных в проверяемом помещении, с контролем (на слух) прохождения всех вызывных сигналов АТС.

Простейшими и наиболее дешевыми **обнаружителями радиоизлучений закладных устройств являются индикаторы электромагнитного поля**, которые световым или звуковым сигналом сигнализируют о наличии в точке расположения антенны электромагнитного поля с напряженностью выше пороговой (фоновой). Более сложные из них - частотомеры обеспечивают, кроме того, измерение несущей частоты наиболее "сильного" в точке приема сигнала.

Для **обнаружения излучений закладных устройств в ближней зоне могут использоваться и специальные приборы, называемые интерсепторами.** Интерсептор автоматически настраивается на частоту наиболее мощного сигнала и осуществляет его детектирование. Некоторые интерсепторы позволяют не только производить автоматический или ручной захват радиосигнала, осуществлять его детектирование и прослушивание через динамик, но и определять частоту обнаруженного сигнала и вид модуляции.

Чувствительность обнаружителей поля мала, поэтому они позволяют обнаруживать излучения радиозакладок в непосредственной близости от них.

Существенно лучшую чувствительность имеют **специальные (профессиональные) радиоприемники с автоматизированным сканированием**

радиодиапазона (сканерные приемники или сканеры). Они обеспечивают поиск в диапазоне частот, перекрывающем частоты почти всех применяемых радиозакладок - от десятков кГц до единиц ГГц. Лучшими возможностями по поиску радиозакладок обладают анализаторы спектра. Кроме перехвата излучений закладных устройств они позволяют анализировать и их характеристики, что немаловажно при обнаружении радиозакладок, использующих для передачи информации сложные виды сигналов.

Возможность сопряжения **сканирующих приемников с переносными компьютерами послужило основой для создания автоматизированных комплексов для поиска радиозакладок** (так называемых, программно-аппаратных комплексов контроля). Кроме программно-аппаратных комплексов, построенных на базе сканирующих приемников и переносных компьютеров, для поиска закладных устройств используются и специально разработанные многофункциональные комплексы, такие, например, как "OSCOR-5000".

Специальные комплексы и аппаратура для контроля проводных линий позволяют проводить измерение параметров (напряжений, токов, сопротивлений и т.п.) телефонных, слаботочных линий и линий электропитания, а также выявлять в них сигналы закладных устройств.

Обнаружители пустот позволяют обнаруживать возможные места установки закладных устройств в пустотах стен или других деревянных или кирпичных конструкциях.

Большую группу образуют **средства обнаружения или локализации закладных устройств по физическим свойствам элементов электрической схемы или конструкции**. Такими элементами являются: полупроводниковые приборы, которые применяются в любых закладных устройств, электропроводящие металлические детали конструкции и т.д. Из этих средств наиболее достоверные результаты обеспечивают средства для обнаружения полупроводниковых элементов по их нелинейным свойствам - нелинейные радиолокаторы.

Принципы работы **нелинейных радиолокаторов** близки к принципам работы радиолокационных станций, широко применяемых для радиолокационной разведки объектов. Существенное отличие заключается в том, что если приемник радиолокационной станции принимает отраженный от объекта зондирующий сигнал (эхо-сигнал) на частоте излучаемого сигнала, то приемник нелинейного локатора принимает 2-ю и 3-ю гармоники отраженного сигнала. Появление в отраженном сигнале этих гармоник обусловлено нелинейностью характеристик полупроводников.

Металлоискатели (металлодетекторы) реагируют на наличие в зоне поиска электропроводных материалов, прежде всего металлов, и позволяют обнаруживать корпуса или другие металлические элементы закладки.

Переносные рентгеновские установки применяются для просвечивания предметов, назначения которых не удается выявить без их разборки, прежде всего тогда, когда разборка невозможна без разрушения найденного предмета.

3. Порядок проверки технических средств и выделенных помещений на наличие электронных устройств негласного получения информации.

Выявление внедренных на объекты электронных устройств перехвата информации достигается проведением специальных проверок, которые проводятся при проведении аттестации помещений, предназначенных для ведения конфиденциальных переговоров, а также - периодически.

В зависимости от целей, задач и используемых средств можно выделить следующие виды специальных проверок:

- специальное обследование выделенного помещения;

- визуальный осмотр выделенного помещения;
- комплексная специальная проверка помещения;
- визуальный осмотр и специальная проверка новых предметов (подарков, предметов интерьера, бытовых приборов и т.п.) и мебели, размещаемых или устанавливаемых в выделенном помещении;
- специальная проверка радиоэлектронной аппаратуры, устанавливаемой в выделенном помещении;
- периодический радиоконтроль (радиомониторинг) выделенного помещения;
- постоянный (непрерывный) радиоконтроль помещения;
- специальная проверки проводных линий;
- проведение тестового "прозвона" всех телефонных аппаратов, установленных в проверяемом помещении, с контролем (на слух) прохождения всех вызывных сигналов АТС.

Периодичность и виды проверок помещений с целью выявления в них закладных устройств зависят от степени важности помещений и порядка допуска в них посторонних лиц.

Специальное обследование и визуальный осмотр выделенного помещения проводятся без применения технических средств. Остальные же виды проверок требуют использования тех или иных специальных средств контроля.

Специальные обследования помещений проводятся после окончания строительства объекта или после проведения капитального ремонта в них, а также периодически. Для проведения специальных обследований должны привлекаться соответствующие специалисты.

Визуальный осмотр помещений проводится перед началом и после завершения служебных совещаний, а также в начале и после завершения рабочего дня. Если проверка проводится вечером, то после ее завершения помещение должно быть закрыто и опечатано, а ключи в опечатанном тубусе должны сдаваться под охрану. Данный вид проверки кабинетов руководящего состава целесообразно поручать их секретарям, так как они могут наиболее быстро выявить новые предметы, появившиеся в кабинете. Проверку помещений для проведения служебных совещаний целесообразно поручать специалистам.

При проведении визуального осмотра выделенных помещений особое внимание уделяется местам, куда можно быстро и скрытно установить закладное устройство. Этот вид контроля позволяет выявить закладки, оставляемые посетителями в легко доступных местах: под столешницами, под сидениями стульев, в различных щелях, за картинами, за батареями, за мебелью, за шторами и т. д.

Визуальный осмотр и специальная проверка новых предметов и мебели проводится перед их установкой в выделенном помещении. Как правило, проверяются предметы и мебель, приобретаемые по предварительному заказу или доставляемые фирмой-посредником, а также представительские подарки и сувениры. Для проведения проверки используются нелинейные локаторы и рентгеновские комплексы.

С целью обнаружения звуко- и видеозаписывающей аппаратуры, а также радиозакладок может поводиться досмотр специальная проверка посетителей и их вещей.

Специальная проверка радиоэлектронной аппаратуры, в том числе ПЭВМ и телефонных аппаратов, проводится после их закупки или ремонта. Для проведения проверки применяются рентгеновские комплексы, радиоизмерительная техника и специальные программно-аппаратные комплексы контроля.

Специальная проверка проводных линий осуществляется после окончания строительства объекта или после проведения его капитального ремонта, а также периодически с целью обнаружения несанкционированных подключений к линиям средств съема информации. Для проведения проверки должны привлекаться соответствующие специалисты.

Радиоконтроль выделенных помещений проводится с целью обнаружения

активных радиозакладок с использованием сканерных приемников или программно-аппаратных комплексов контроля. Он организуется периодически, при проведении наиболее важных мероприятий (совещаний, заседаний и т.п.), или непрерывно (постоянно). При этом средства контроля могут располагаться вне контролируемых помещений.

Тестовый "прозвон" телефонных аппаратов проводится при установке нового телефонного аппарата или телефонного аппарата после ремонта, а также периодически. "Прозвон" необходимо проводить с радиотелефона или телефонного аппарата, установленного в другом помещении. При наборе номера проверяемого телефонного аппарата осуществляется контроль (на слух) прохождения всех вызывных сигналов АТС.

Если обнаружено подавление (непрохождение) одного-двух вызывных звонков у контролируемого телефонного аппарата, то возможно, что в его корпусе или телефонной линии установлено закладное устройство типа "телефонного уха" и необходимо проводить специальную проверку телефонной линии и телефонного аппарата.

Комплексная специальная проверка помещений проводятся после окончания строительства объекта или после проведения капитального ремонта в них, при проведении аттестации помещений, а также периодически. Это наиболее полный вид проверки. Для проведения таких специальных проверок используется весь арсенал технических средств контроля.

Специальные проверки должны проводить **специалисты организаций, имеющих лицензии уполномоченных органов.**

При организации специальной проверки можно выделить три этапа: подготовка к проведению проверки, непосредственное проведение проверки и оформление результатов проверки.

Первый вид работ включает специальное обследование и проверку с использованием технических средств поверхности стен, потолков, полов, дверей и оконных рам, а также мебели, предметов интерьера, сувениров и т.п. Для его проведения необходимы следующая аппаратура и техника: нелинейный локатор, переносной рентгеновский комплекс, металлоискатель, обнаружитель пустот, индикатор электромагнитного поля, радиочастотомер, а также вспомогательное досмотровое оборудование.

Второй вид работ связан с визуальным осмотром и проверкой с использованием технических средств электронных приборов. При этом используются: переносной рентгеновский комплекс, индикатор электромагнитного поля, радиочастотомер и набор луп.

Третий вид работ включает визуальный осмотр и проверку с использованием технических средств проводных линий (электросети, абонентской телефонной сети, системы часофикации, систем пожарной и охранной сигнализации и т.д.). Для проверки используются средства контроля проводных линий, а также индикатор электро-магнитного поля и радиочастотомер.

Четвертый вид работ предусматривает радиоконтроль (радиомониторинг) помещений. Он проводится с использованием программно-аппаратных комплексов контроля или обычных сканерных приемников. Для анализа структуры сигналов применяются анализаторы спектра.

Рассмотренные виды работ могут проводиться параллельно несколькими группами или последовательно.

Специальное проверка помещения начинается с его тщательного осмотра.

При визуальном осмотре применяется вспомогательное оборудование: фонари, досмотровые зеркала и эндоскопы, а также набор луп.

Фонари применяются для осмотра плохо освещаемых мест.

Досмотровые зеркала применяются для осмотра труднодоступных мест (мебельных ниш, вентиляционных и других отверстий строительных конструкций, люстр и т.п.).

Типовой досмотровой комплект зеркал включает в себя сменные зеркала различных размеров и конфигурации и телескопическую штангу, на конце которой закрепляется фонарь и одно из зеркал.

При визуальном осмотре высоко расположенных объектов (люстр и других светильников, верхних полок шкафов и т.п.) могут использоваться стремянки.

Для поиска малогабаритных закладок в местах, не просматриваемых с помощью зеркал, применяются волоконно-оптические эндоскопы, которые используются для скрытного наблюдения.

Лупы применяются для детального анализа обследуемых предметов.

Визуальный осмотр должен начинаться с протоколирования и фотографирования мест расположения всех предметов в обследуемом помещении. При этом используются подготовленные планы помещений, на которых уточняется расположение мебели, предметов интерьера и аппаратуры и т.д. Записываются их наименование, серийные (инвентарные) номера, номера пломб и печатей и т.п.

После составления протокола и фотографирования мест расположения всех предметов необходимо удалить из контролируемого помещения (или собрать в определенном месте помещения) все электронные устройства: ПЭВМ, телевизоры, магнитофоны, радиоаппаратуру и т.п.

В целях обеспечения полноты визуального контроля целесообразно проводить его по определенной схеме: от двери по часовой стрелке и от периферии к центру помещения.

Осматриваются все поверхности стен, потолков, полов, дверей, оконных рам. Внимательно осматриваются мебель, картины, сувениры и игрушки, цветочные горшки, система отопления, электросеть, системы пожарной, охранной сигнализации и пожаротушения, радиоэлектронная аппаратура, электроприборы, оргтехника, радиотрансляционная сеть, система часофикации, телефонная сеть, урны для мусора и т.д.

Осмотр необходимо проводить последовательно, методично, просматривая фрагмент за фрагментом.

При осмотре стен особое внимание обращается на наличие "свежих" царапин на обоях возле электрических и телефонных розеток, выключателей освещения, участков стены, по тону отличающихся от остальной поверхности (следы свежей краски, потемнение (посветление) обоев и т.д.).

Бра и электрические розетки снимаются, разбираются и осматриваются. При этом необходимо соблюдать правила электробезопасности. При осмотре они должны отключаться от электросети. Осматриваются не только сами электрические розетки, электрощиты, но и ниши, в которых они установлены. При осмотре обращается внимание на подводящие провода электрощитов и розеток.

Особое внимание уделяется осмотру вентиляционных решеток и коробов. Проверяется крепление решетки, и не снималась ли она. Вентиляционные короба могут осматриваться с использованием эндоскопов или с использованием досмотровых зеркал. В последнем случае необходимо снять вентиляционные решетки.

При осмотре системы отопления необходимо осмотреть пространство за решетчатым ограждением, между ребер батарей и места входа труб в стены или пол (потолок).

Особое внимание обращается на пылевые следы смещения картин, настенных часов или других предметов. Настенные часы осматриваются как снаружи, так и внутри. При осмотре картин необходимо внимательно осмотреть их обратную сторону.

Рамы окон осматриваются при их открытом и закрытом положении. Осматриваются места между рамами и оконными проемами. При необходимости производится осмотр используемого уплотнителя. Особое внимание уделяется осмотру карнизов и штор.

При осмотре пола внимание обращается на отслоение паркетин и царапины на

них, на отслоения или вздутости линолеума (коврового покрытия), а также царапины в местах крепления и отслоение плинтусов, следы свежей краски на них.

Осматриваются (внутри и днища) урны, напольные вазы и другие напольные предметы интерьера.

Осматривая крашенный (или поклеенный) потолок необходимо обратить внимание на наличие участков, по тону отличающихся от остальной поверхности (следы свежей краски, изменение цвета обоев), а также на царапины в местах крепления, отслоение потолочных плинтусов, следы свежей краски на них.

При осмотре подвесных потолков внимание обращается на царапины и нарушения в креплении плиток. Целесообразно снять несколько плиток и осмотреть (в том числе и с использованием досмотровых зеркал) пространство между основным и подвесным потолками.

Датчики охранной и пожарной сигнализации осматриваются внутри. Если они опломбированы, то проверяется целостность пломб.

Люстры осматриваются внутри при отключенном электропитании.

Перед осмотром мебели обращается внимание на изменение ее расположения от ранее установленного порядка (смещена, повернута, переставлена местами друг относительно друга и т.д.).

Мебель при осмотре отодвигается от стен и друг друга. Внимательно осматриваются пол под диванами, шкафами, сейфами, днища шкафов, диванов, столов, кресел, стульев, складки обивки и соединительные швы мягкой мебели и т.д.

Выдвижные ящики и полки вынимаются и осматриваются. Вынимается и осматривается также содержимое столов, шкафов и т.д.

Труднодоступные и скрытые полости столов, диванов, кресел и т.д. осматриваются с помощью эндоскопов.

Наряду с мебелью проверяются все предметы интерьера, сувениры, игрушки, настольные вазы, пепельницы, зажигалки, цветочные горшки и т.п. При этом особое внимание обращается на царапины, следы свежей краски, клея, сравнительную толщину стенок и объем доступных полостей. Выявляются скрытые полости.

Проверка помещения с использованием специальных технических средств осуществляется или параллельно с проведением визуального осмотра, или после него. При этом обязательно проверяются все выявленные в процессе осмотра подозрительные места и предметы.

Проверку стен, полов и потолков осуществляют с использованием нелинейного локатора. В качестве дополнительных средств применяются обнаружитель пустот и металлоискатель. Если используется нелинейный локатор, осуществляющий прием отраженных сигналов только на второй гармонике, проверку необходимо проводить два раза, первый - с использованием нелинейного локатора, второй - с использованием металлоискателя.

Обнаружение электронного устройства, определение его местоположения и его идентификация осуществляется по методикам, изложенным в третьей главе. Режим работы (включено, выключено) обнаруженного электронного устройства проверяется с использованием индикатора поля. Для определения частоты излучения применяется радиочастотомер.

Подозрительные места, где с использованием нелинейного локатора или металлоискателя обнаружены электронные или металлические объекты, наносятся на схему помещения. При согласии руководства учреждения данные места вскрываются, и осуществляется их осмотр. В противном случае эти работы выполняются при очередном ремонте.

Для проверки небольших по размерам предметов интерьера, сувениров и т.п. наряду с нелинейным локатором и металлоискателем используется портативный переносной рентгеновский комплекс.

Электрические приборы (настольные лампы, нагревательные приборы и т.д.) перед проверкой включаются в сеть, и индикатором поля определяется наличие в них источников радиоизлучения. Затем они обесточиваются, разбираются и осматриваются. В электрические приборы обычно встраиваются некамуфлировонные закладки с питанием от сети 220 В. При этом закладки непосредственно подключаются к проводам электропитания приборов. Разбираются и проверяются не только сами приборы, но и электроудлинители.

Наиболее трудно обнаружить закладки в электронных приборах (оргтехнике, телевизорах, магнитофонах, приемниках, ПЭВМ, телефонных аппаратах и т.д.). Как правило, их техническая проверка осуществляется в специализированных лабораториях. Однако в ряде случаев проверка может проходить и непосредственно на контролируемом объекте.

Перед осмотром электронные приборы включаются, в и индикатором поля определяется наличие в них источников радиоизлучения, затем они обесточиваются и разбираются.

Визуальный осмотр блоков и плат приборов осуществляется с помощью лупы.

При наличии снимков типовых блоков (печатных плат) аналогичных приборов проводится их сравнение с наблюдаемыми.

Особое внимание уделяется наличию в приборе небольших предметов неизвестного назначения (подключенных, как правило, к блоку питания аппаратуры), дополнительных плат, изменение в штатных печатных платах или появление в электронном приборе дополнительных радиоэлементов; наличию на платах мест со следами "свежей" (отличной от заводской) пайки, отличие элементов (конденсаторов, резисторов и т.п.) от заводских (по внешнему виду, размерам, отсутствию соответствующих надписей и т.п.)

При проверке телефонных аппаратов разбираются и осматриваются не только их корпуса, но и телефонные трубки и телефонные коробки. Особое внимание уделяется наличию в корпусе аппарата, телефонной трубке или телефонной розетке элементов (деталей) неизвестного назначения, подключенных (последовательно или параллельно) к телефонной линии. Внимательно осматриваются внешний вид и соответствующие надписи на всех конденсаторах, микрофонном и телефонном капсюлях.

При предположительном обнаружении в том или ином предмете или элементе схемы (блока) прибора акустической закладки они внимательно осматриваются с помощью лупы. При детальном осмотре особое внимание уделяется наличию в их корпусах (стенках) небольших (диаметром около 1 мм) отверстий под микрофоны.

Подозрительные неразборные блоки, платы и элементы схем электронных приборов проверяются с использованием рентгеновских комплексов.

Осмотр и проверку подозрительных предметов и элементов желательно проводить таким образом, чтобы не стереть или повредить возможно оставленные противником (преступником) отпечатки пальцев.

Перед изъятием подозрительных предметов для специальной технической проверки производится их фотографирование и запоминается (протоколируется) их местоположение. При этом необходимо обратить внимание на возможные метки, оставляемые с целью фиксирования места размещения предметов, имеющих устройства съема информации.

После проведения проверки электронная аппаратура, электрические приборы, щитки, розетки, вентиляционные решетки и т.д. представителям проверяющей организации опечатываются специальными пломбами или маркируются специальными метками, в том числе ультрафиолетовыми. Использование ультрафиолетовых меток является предпочтительным, так как они являются невидимыми и обнаружить их можно только при облучении ультрафиолетовыми источниками света. Виды и места установки меток указываются в пояснительной записке к плану помещения. При очередной проверке

проверяется, вскрывались ли эти приборы и блоки.

Проверка проводных линий (электросети, абонентской телефонной сети, системы часофикации, систем пожарной и охранной сигнализации и т.д.) осуществляется или параллельно с проведением проверки помещения, или после ее проведения.

Проверка начинается с визуального осмотра каждой линии в соответствии с ее схемой. Особое внимание уделяется осмотру всех распределительных коробок, щитов, параллельных отводов, блокираторов и т.п. В процессе осмотра схемы проводных линий уточняются, на них наносятся не указанные отводы, распределительные коробки и т.п.

После визуального осмотра осуществляется проверка линий с использованием технических средств. Тот или иной метод проверки проводных линий зависит от принципов работы и характеристик используемых средств контроля.

Проверку проводных линий целесообразно осуществлять в следующей последовательности: вначале проверяется силовая сеть, затем - линии телефонной связи и в конце - линии пожарной и охранной сигнализации и т.д.

При проверке силовых линий необходимо строго соблюдать правила электробезопасности.

Вначале осуществляется проверка каждой линии на наличие в ней высокочастотных сигналов, модулированных информационным сигналом.

Слаботочные линии дополнительно проверяются на наличие в них информационных низкочастотных сигналов.

При обнаружении сигналов, передаваемых средствами съема информации, их поиск и локализация производится путем подключения прибора к различным точкам силовой сети или слаботочной проводной линии с одновременным контролем уровня прослушиваемых сигналов и визуальным осмотром подозрительных участков.

После проверки линий на наличие в них высокочастотных и низкочастотных сигналов проводится их проверка на наличие подключенных средств съема информации с использованием нелинейного локатора проводных линий, а затем производится измерение параметров линий.

В обследуемой силовой линии вычленяется проверяемый участок, который отключается от источника питающего напряжения. Наиболее удобно отключение линии проводить на распределительном щите. От обследуемой линии отключаются все электрические приборы (легальные нагрузки). Из люстр, бра необходимо вывернуть все лампы, все выключатели устанавливаются во включенное положение.

К одним концам проверяемого участка силовой линии подключается нелинейный локатор, а к другим - испытательная (эквивалентная) нагрузка.

При проверке телефонной линии необходимо ее разъединить и отключить от нее телефонный аппарат, подключив вместо него эквивалентную нагрузку. Разъединение (отключение телефонной линии) целесообразно проводить на вводной распределительной коробке (щитке) здания. Подключение локатора к линии осуществляется в месте ее разъединения.

В случае если после проведения технической проверки и визуального осмотра в линии не обнаружено подключенных средств съема информации, то проводится измерение ее параметров (активного и реактивного сопротивлений, емкости и индуктивности). Причем, измерения проводятся при разомкнутом и замкнутом (накоротко) состояниях линии. Результаты измерений заносятся в таблицу.

При измерении параметров телефонной линии (после подсоединения телефонного аппарата и подключения линии к АТС) дополнительно фиксируются напряжения при опущенной и поднятой трубке телефонного аппарата. Измерения могут проводиться на вводном распределительном щитке или непосредственно в телефонной розетке. Результаты измерений также заносятся в таблицу.

Полученные результаты измерений параметров проводных линий необходимы для проведения в последующем периодических проверок этих линий.

Радиоконтроль (радиомониторинг) выделенных помещений может проводиться в ходе их специальной проверки, при проведении особоважных мероприятий в этих помещениях, а также постоянно (непрерывно).

Радиоконтроль может проводиться с использованием как обычных сканерных приемников, так и программно-аппаратных комплексов контроля. Наиболее предпочтительным является метод контроля с использованием программно-аппаратных комплексов.

Для повышения эффективности и оперативности контроля его организация начинается за несколько дней до проведения специальной проверки. При этом скрытно осуществляется радиоконтроль электромагнитной обстановки в районе объекта и по его результатам составляется база данных выявленных сигналов.

В случае использования программно-аппаратных комплексов в процессе контроля на жесткий диск ПЭВМ в режиме обновления записывается спектрограмма рабочего диапазона частот (частота и относительный уровень, а также спектры обнаруженных сигналов). По возможности устанавливаются принадлежность и месторасположение источников обнаруженных сигналов.

При проведении специальной проверки программно-аппаратный комплекс (сканерный приемник) разворачивается в выделенном помещении. Устанавливаются внутренняя (в пределах контролируемого помещения) и внешняя (вынесенная на удаление не менее 20 ... 30 м от контролируемого помещения) антенны. Радиоконтроль проводится после специального обследования помещения.

В процессе контроля с использованием активного или пассивных тестов выявляются сигналы, источники которых находятся в выделенном помещении.

Локализация источников сигналов, выявленных в контролируемом помещении, может проводиться как с использованием программно-аппаратного комплекса в соответствующем режиме работы, так и с использованием других средств (например, переносных сканерных приемников, индикаторов поля, радиочастотомеров и т.д.).

Периодический радиоконтроль наиболее целесообразно организовывать при проведении особо важных мероприятий (совещаний, переговоров, встреч и т.п.). В этом случае пункт радиоконтроля обычно размещается в специально выбранном помещении на объекте, а в контролируемом помещении скрытно устанавливаются широкополосная антенна и выносной микрофон, который подключается к бесшумному коррелятору комплекса контроля. Пункт радиоконтроля также может быть развернут в автомашине, припаркованной недалеко от объекта.

Но наиболее эффективна организация постоянного (круглосуточного) радиоконтроля в выделенных помещениях. В этом случае могут быть выявлены не только дистанционно-управляемые радиозакладки, но и закладки с промежуточным накоплением информации, и закладки, использующие для передачи информации аппаратуру быстродействия.

В этом случае в специально оборудованном помещении на объекте разворачивается стационарный пункт радиоконтроля, в состав которого, как правило, включаются один или несколько программно-аппаратных комплексов, позволяющих контролировать все выделенные помещения (например, комплексы КРК, АРК, "Крона", система СОИ и т.п.). На пункте радиоконтроля устанавливается опорная антенна, а в выделенных (контролируемых) помещениях - малогабаритные широкополосные антенны и звуковые колонки или выносные микрофоны (в случае использования в составе комплексов контроля бесшумных корреляторов), которые при установке камуфлируются. Антенны и звуковые колонки (или микрофоны) специально проложенными кабелями соединяются соответственно с блоками высоко-частотного (антенного) или низкочастотного коммутаторов, установленных в помещении стационарного пункта контроля.

В состав комплекса контроля целесообразно включать два приемника, один из

которых использовать в режиме постоянного сканирования заданного диапазона в режиме панорама, а второй - для детального анализ спектров сигналов и их классификации.

Если при проведении радиоконтроля обнаружена передача информации закладкой во время важного особоважного мероприятия, то до принятия решения о дальнейших действиях может быть организована постановка прицельных помех на частоте передачи закладки. Для этих целей может использоваться, например, устройство постановки помех АРК-СП.

Если при проведении специальной проверки обнаружено закладное устройство, руководитель поисковой бригады сообщает об этом факте руководителю учреждения и в территориальный орган ФСБ РФ. Дальнейшие оперативно-следственные действия по изъятию закладки и установлению лиц, внедривших закладку, осуществляют ее представители.

2.9 Лабораторная работа № 9 (2 часа).

Тема: «Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам**»**

2.9.1 Цель работы: изучить методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам

2.9.2 Задачи работы:

1. Способы и принципы работы средств защиты информации от подслушивания.
2. Классификация, сущность и параметры звукоизоляции ограждений, кабин, акустических экранов, глушителей.
3. Способы и средства предотвращения утечки информации с помощью закладных устройств.

2.9.3 Перечень приборов, материалов, используемых в лабораторной работе:

1. Персональный компьютер, специальное ПО

2.9.4 Описание (ход) работы:

1 Способы и принципы работы средств защиты информации от подслушивания

Способы и средства противодействия подслушиванию направлены, прежде всего, на предотвращение утечки информации в акустическом (гидроакустическом, сейсмическом) каналах. Кроме того, для повышения дальности подслушивания применяются составные каналы утечки информации, содержащие наряду с акустическими также радиоэлектронные (с использованием закладных устройств) и оптические (с лазерными микрофонами). Поэтому защита информации от подслушивания включает способы и средства блокирования любых каналов, с помощью которых производится утечка акустической информации.

В соответствии с общими методами защиты информации для защиты от подслушивания применяются следующие способы:

1) информационное скрытие, предусматривающее:

- техническое закрытие и шифрование семантической речевой информации в функциональных каналах связи;
- дезинформирование;

2) энергетическое скрытие путем:

- звукоизоляции акустического сигнала;
- звукопоглощения акустической волны;
- глушения акустических сигналов;
- зашумления помещения или твердой среды распространени другими широкополосными звуками (шумами, помехами), обеспечивающими маскировку акустических сигналов;

3) обнаружение, локализация и изъятие закладных устройств.

Способы и средства информационного скрытия речевой информации от подслушивания

Информационное скрытие речевой информации обеспечивается техническим закрытием (аналоговым скремблированием) и шифрованием сигналов речевой информации, передаваемых по кабелям и радиоканалам.

При аналоговом скремблировании изменяются характеристики исходного речевого сообщения таким образом, что преобразованное сообщение становится нераспознаваемым «на слух», но занимает ту же частотную полосу. Это позволяет передавать скремблированные сигналы по обычным коммерческим телефонным каналам связи..

Классификация способов технического закрытия приведена на рис. 4.1.

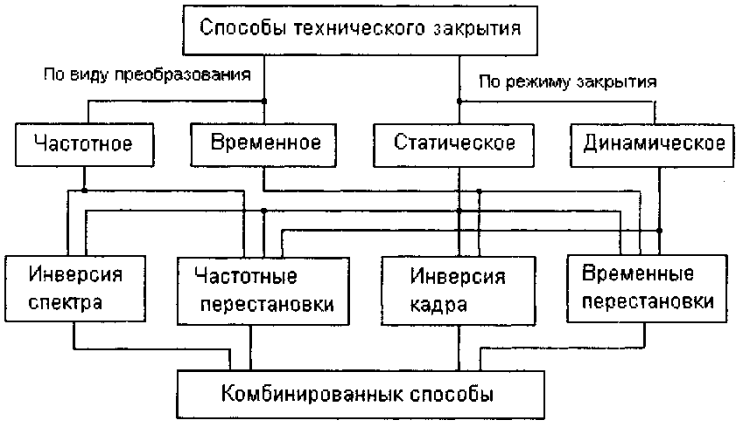


Рис. 4.1.- Классификация способов технического закрытия

В скремблере, реализующем инверсию спектра и называемым также маскиратором, осуществляется преобразование речевого спектра путем поворота частотной полосы речевого сигнала вокруг некоторой средней точки спектра fo (рис. 4.2). В этом случае достигается эффект преобразования низких частот в более высокие и наоборот.

Этот способ обеспечивает невысокий уровень закрытия, так как при перехвате достаточно легко определяется значение частоты fo инверсии спектра речевого сигнала.

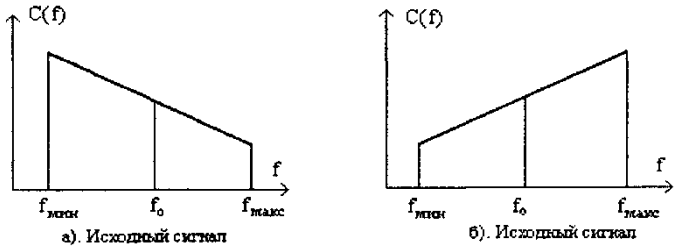


Рис.4.2. - Принципы инверсии частотного спектра речевого сигнала

В скремблере, выполняющего частотные перестановки, спектр исходного речевого сигнала разделяется на несколько частотных полос равной ширины (в современных моделях число полос может достигать 10-15), производится их перемешивание по некоторому алгоритму - ключу (рис. 4.3). При приеме спектр сигнала восстанавливается в результате обратных процедур.

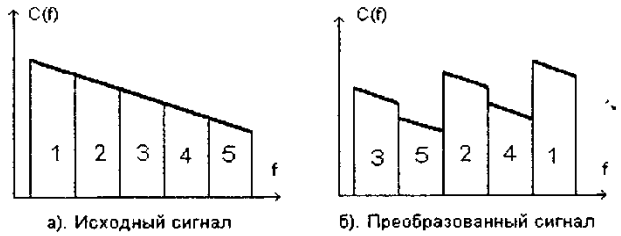


Рис. 4.3. Принципы частотной перестановки

Изменение ключа в ходе сеанса связи в скремблерах с динамическим закрытием позволяет повысить степень закрытия, но при этом требуется передача на приемную сторону сигналов синхронизации, соответствующих моментам смены ключа.

Другие виды преобразования носителя речевой информации реализуют временные способы технического закрытия с более высоким уровнем защиты информации. Инверсия кадра обеспечивается путем предварительного запоминания в памяти передающего скремблера отрезка речевого сообщения (кадра) длительностью Тк и считывание его (с передачей в телефонную линию) с конца кадра - инверсно. При приеме кадр речевого сообщения запоминается и считывается с устройства памяти в обратном порядке, что обеспечивает восстановление исходного сообщения. Для достижения неразборчивости речи необходимо, чтобы продолжительность кадра была не менее 250 мс. В этом случае суммарная продолжительность запоминания и инверсной передачи кадра составляет примерно 500 мс, что может создать заметные задержки сигнала при телефонном разговоре.

В скремблерах с временной перестановкой кадр речевого сообщения делится на отрезки (сегменты) длительностью τс каждый. Последовательность передачи в линию сегментов определяется ключом, который должен быть известен приемной стороне (рис. 4.4).

Изменением ключа в ходе сеанса связи в скремблерах с динамическим закрытием можно существенно повысить уровень защиты речевой информации. Остаточная разборчивость зависит от длительности кадра и с увеличением последнего уменьшается.

Вследствие накопления информации в блоке временного преобразования появляется задержка между поступлением исходного речевого сигнала в передатчик и восстановлением его в приемнике. Эта задержка неприятно воспринимается на слух, если превышает 1-2 с. Поэтому Тк выбирают равной (4-16) τс.

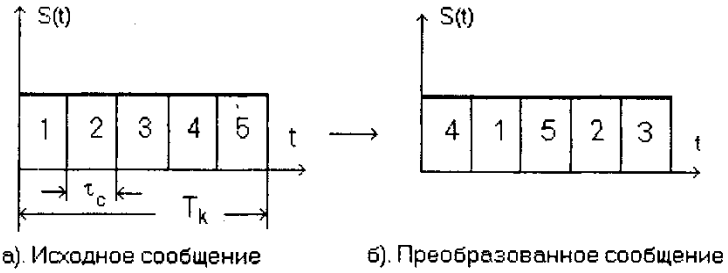


Рис. 4.4. Принципы временной перестановки

Используя комбинацию временного и частотного скремблирования, значительно повышают степень закрытия речи.

В комбинированном (частотно-временном) скремблере исходное сообщение разделяется на кадры и сегменты, которые запоминаются в памяти скремблера. При формировании передаваемого сообщения производятся временные перестановки сегментов кадра и перестановки полос спектра речевого сигнала каждого сегмента, Если при этом обеспечить динамическое изменение ключа временной и частотной перестановки, то уровень защиты такого комбинированного технического закрытия может не уступать цифровому шифрованию. Однако сложность реализации такого способа и

требования к качеству передачи синхроимпульсов между скремблерами телефонных абонентов также высоки.

К достоинствам наиболее широко используемых скремблеров относится простота технической реализации и, как следствие, низкая стоимость и малые габариты, а также возможность их эксплуатации практически на любых каналах связи, предназначенных для передачи речевых сообщений. Основной недостаток простых скремблеров - относительно низкая стойкость закрытия информации. Кроме того, скремблеры, за исключением простейшего (с частотной инверсией), вносят искажения в восстановленный речевой сигнал. Границы частотных полос и временных сегментов нарушают целостность исходного сигнала, что приводит к появлению внеполосных составляющих. Нежелательное влияние оказывают и групповые задержки составляющих речевого сигнала.

Однако, несмотря на указанные недостатки, методы временного и частотного скремблирования, а также их различные комбинации, исключают понимание речевой информации на «слух». Для восстановления речи требуется запись закрытого сообщения на аудиомагнитофон, длительная и трудоемкая работа с использованием дорогостоящей аппаратуры. Поэтому аналоговое скремблирование успешно используется в коммерческих каналах связи для защиты конфиденциальной информации.

Альтернативой скремблированию является цифровое шифрование речевых сигналов, предварительно преобразованных в цифровую форму. При аналого-цифровом преобразовании амплитуда сигнала измеряется через равные промежутки времени, называемые шагом дискретизации. Для того чтобы цифровой речевой сигнал имел качество не хуже телефонного, шаг дискретизации не должен превышать 160 мкс, а количество уровней квантования амплитуды речевого сигнала - не менее 128. В этом случае один отсчет амплитуды кодируется 7 битами, скорость передачи превышает 43 кбит/с, а ширина спектра дискретного двоичного сигнала равна сумме полос 14 стандартных телефонных каналов.

Для передачи речи в цифровой форме по стандартному телефонному каналу необходимо резко сократить полосу речевого сигнала. Эта проблема решается в устройстве, называемом вокодером. В передающей части вокодера из речевого сигнала выделяются медленно изменяющиеся информационные параметры спектра речи, основной тон вокализованных (звонких) звуков и переходы тон-шум глухих звуков.

Вокодеры различаются в зависимости от выделяемых параметров. Распространены полосные вокодеры и вокодеры с линейным предсказанием.

В полосном вокодере анализируется форма речевого сигнала с периодом анализа 10-30 мс, выделяются и передаются по телефонному каналу в цифровом виде: значения амплитуд ограниченного числа частотных полос спектра речевого сигнала, величины периода основного тона для вокализованных звуков и решение тон/шум, соответствующее наличию или отсутствию вокализованного участка в речевом сигнале. В приемном вокодере синтезируются звуки с переданными параметрами.

В большинстве практических случаев анализ речевых сигналов проводится с периодом 20 мс для 16-20 частотных полос, выделяемых полосовыми фильтрами, а параметры речи по телефонному каналу передаются со скоростью 2400 бит/с. При снижении требований к качеству синтезированной речи скорость передачи речевой информации может быть уменьшена до 1200-1800 бит/с.

В вокодерах с линейным предсказанием исходный речевой сигнал аппроксимируется кусочно-линейной функцией, каждый текущий отчет которой является линейной функцией n предыдущих отчетов. В этих вокодерах речевая информация передается величиной амплитуды, значениями коэффициентов линейного предсказания, периодом основного тона и решением о тоне или шуме. Скорость передачи речевой информации в широко распространенных вокодерах с линейным предсказанием для n=10 составляет 2400 бит/с, но существует возможность снижения ее до 800 бит/с и менее с допустимой потерей качества речи.

Вокодеры для телефонной закрытой связи со скоростью передачи 4800 бит/с обеспечивают слоговую разборчивость до 93% (словесная разборчивость достигает 99%) при удовлетворительной узнаваемости абонента. В телефонных каналах низкого качества скорость информационного потока на выходе вокодера снижают до 2400 бит/спри сохранении хорошей разборчивости, но низкой узнаваемости голоса абонента.

Шифрование речевой информации в цифровой форме производится известными методами (заменой, перестановками, аналитическими преобразованиями, гаммированием и др.).

Алгоритм DES, применяемый в США с 1976 года, является суперпозицией шифров, состоящего из 16-ти последовательных циклов, в каждом из которых сочетаются подстановки и перестановки. Он реализуется программно, обеспечивает скорость передачи 10-200 кБ/с и криптостойкость 10 операций при длине ключа 56 бит.

Алгоритм криптографического преобразования, определяемый ГОСТ 28147-89, обладает криптостойкостью, оцениваемой 10 операций (длина ключа 256 бит), обеспечивает скорость шифрования 50-70 кБ/с и реализуется в основном аппаратно.

Основным достоинством систем цифрового шифрования речевого сигнала является высокая надежность закрытия информации, так как перехваченный сигнал представляет из себя случайную цифровую последовательность. Для восстановления из нее исходного сообщения необходимо знать криптосхему шифратора и устройство вокодера.

Недостатком устройств цифрового шифрования речи являются необходимость использования модемов, техническая сложность и относительно большие габариты шифраторов, неустойчивая работа устройств в каналах с большим затуханием сигнала и с высоким уровнем помех.

Сравнительные возможности различных методов закрытия речи указаны на рис. 4.5.

Под тактическим (низким или закрытием с временной стойкостью) понимается уровень, обеспечивающий защиту информации от подслушивания посторонними лицами в течение от минут до нескольких дней. Для дешифрования перехваченных сообщений со стратегическим (высоким, с гарантированной стойкостью) уровнем защиты информации высококвалифицированному, технически хорошо оснащенному специалисту потребуется от нескольких месяцев до многих лет.

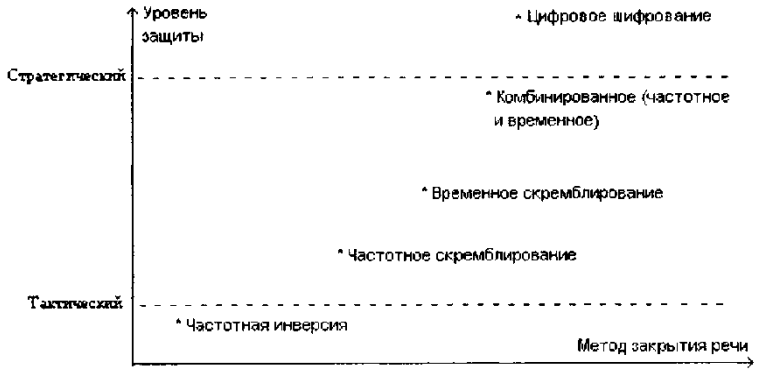


Рис. 4.5. Уровни защиты различных методов закрытия речевой информации

Характеристики отечественных образцов скремблеров, обеспечивающих тактическую стойкость, приведены в табл. 4.1.

Таблица 4.1 - Характеристики отечественных образцов скремблеров, обеспечивающих тактическую стойкость

Параметры	Изделие, фирма				
	«Орех-». Анкад	«Базальт»Прогресс	«Уза». ПНИЭИ	СТА 1000, Герос	SCR M1.2, Синтез
Режим работы	дуплекс	п/дуплекс	п/дуплекс	п/дуплекс	п/дуплекс

Кол-во уровнен защиты	3	1	1	1	1
Разрядность ключа	128 бит	9-16	16	1-16	7
Кол-во комбинации ключа	1036	Ю16	1016	1025	107
Время установления закрытой связи, сек	1-7	2-8	8	-	-
Средняя разборчивость речи	90%	-	95%	-	-
Время задержки сигнала.сек	0.32	0.32	до 0.9	032	До1
Размеры, мм	190х296х45	210х2-90х45	-	330х260х65	275х290х65
Масса, кг	2	2.5	8.2	3	3.2

Например, закрытие речевой информации скремблером тактической стойкости с наиболее высокими показателями «Орех-А» достигается за счет временных перестановок, инверсии спектра сигнала и преобразования временного масштаба, разрушающего непрерывность речевого сигнала.

Криптографическая стойкость обеспечивается трехуровневой ключевой системой, включающей в себя:

- пароль, известный абонентам, входящим в связь;
- мастер-ключ, используемый при формировании ключевой информации в процессе установления соединения;
- сеансовый ключ, генерируемый с использованием физического датчика случайных чисел.

Характеристики средств гарантированной защиты приведены в табл. 4.2.

Таблица 4.2. - Характеристики средств гарантированной защиты

Параметры	Изделие, фирма			
	«Орех-IV». Анкад	АТ-2400. Анкорд	«Разбег-К». ПНИЭИ	«Гамма». НТЦ ФАПСИ
Режим работы	Дуплекс	Дуплекс	Дуплекс	Дуплекс
Скорость передачи, бит/с	9600	2400	2400	2400. 4800, 9600
Средняя слоговая разборчивость речи	90-95%	Высокая	85%	Высокая

При использовании алгоритмов DES или ГОСТ 28147-89 на получение исходного сообщения потребуется до нескольких десятков лет.

Скремблеры выпускаются в виде подставок под телефонный аппарат («Орех-А, «Орех-IV») или отдельных блоков. Телефонный скремблер «Уза» размещается в чемодане типа «кейс» и подключается к телефонной линии напрямую или через акустический соединитель.

При применении скремблеров необходимо иметь ввиду, что скремблер должен

иметь 2 сертификата: от Министерства связи - на средство связи и от ФАПСИ - на средство обеспечения безопасности информации. НТЦ ФАПСИ созданы аппараты для гарантированной защиты информации, передаваемой средствами стационарной и подвижной связи:

- «Альфа» - аппарат шифрования речевой факсимильной и документальной информации для подвижной радиосвязи (скорость передачи 2400, 4800, 9600 бит/с, 360х280х100 мм, 8.5 кг);
- «Эпсилон» - носимый аппарат шифрования информации (4800 бит/с, 232х263х113 мм, 5.6 кг);
- «Сигма» - малогабаритный аппарат шифрования речевой информации (1200 бит/с, 156х65х261 мм, 2 кг);
- «Омега» - малогабаритный аппарат шифрования речевой, факсимильной и документальной информации (1200, 2400 бит/с, 150х74х256 мм. 3.5 кг).

Эти аппараты применяют ключ длиной 256 бит.

Дезинформирование возможно как в акустическом, так и составном каналах утечки информации. Например, после обнаружения закладки можно ее не изымать, а использовать для дезинформирования злоумышленников.

2 Классификация, сущность и параметры звукоизоляции ограждений, кабин, акустических экранов, глушителей

Энергетическое скрытие акустических сигналов в соответствии с рассмотренными методами защиты информации обеспечивается путем применения способов и средств, уменьшающих энергию носителя или увеличивающих энергию помех.

Простейшим способом первого метода является уменьшение громкости речи во время разговора на конфиденциальные темы. Однако это возможно, если количество собеседников мало. В иных случаях применяют звукоизоляцию, звукопоглощение и глушение звука. Второй метод предусматривает применение активных средств — генераторов акустических помех.

Звукоизоляция направлена на локализацию источников акустических сигналов в замкнутом пространстве внутри контролируемых зон. Основное требование к ней - за пределами этой зоны соотношение сигнал/помеха не должны превышать максимально-допустимые значения, исключающие добывание информации злоумышленниками. Учитывая, что средняя громкость звука говорящего в помещении составляет около 50-60 дБ, то в зависимости от категории помещения его звукоизоляция должна быть не менее норм, приведенных в табл.4.3.

Таблица 4.3 –Нормы звукоизоляции помещений по категориям

Частота(Гц)	Категория выделенного помещения.дБ		
	I	II	III
500	53	48	43
1000	56	51	46
2000	56	51	46
4000	55	50	45

При этих значениях звукоизоляции уровни звука вне помещений на фоне акустических шумов не обеспечивают подслушивание разговоров.

Звукоизоляция обеспечивается с помощью архитектурных и инженерных конструкций: ограждений, экранов, кабин, кожухов (рис. 4.6).

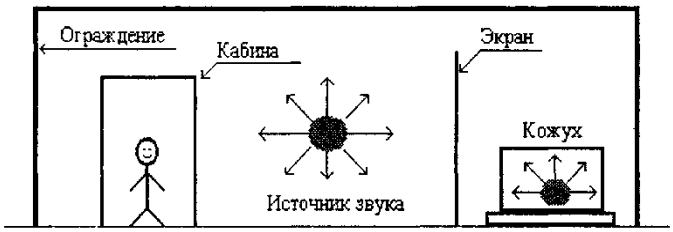


Рис.4.6. Основные средства звукоизоляции

Звукоизоляция оценивается величиной ослабления R в дБ акустической волны, равного R=10·lgPпад /Рпр, где Рпад - мощность падающей на средство звукоизоляции акустической волны, Рпр - мощность акустической волны, прошедшей через это средство. При падении акустической волны на границу поверхностей с различными удельными плотностями большая часть падающей волны отражается. Меньшая часть волны проникает в материал звукоизолирующей конструкции и распространяется в нем, теряя свою энергию в зависимости от длины пути и его акустических свойств материала. Под действием акустической волны звукоизолирующая поверхность совершает сложные колебания, также поглощающие энергию падающей волны.

Характер этих поглощений определяется соотношением частот падающей акустической волны и спектральных характеристик (распределения частот) поверхности средства звукоизоляции. В области резонансных частот (до 25-45 Гц) средств звукоизоляции ослабление зависит в основном от внутреннею трения в звукоизолирующем материале, на более высоких частотах - от его поверхностной плотности, измеряемой в кг на 1 м2 поверхности. С учетом действующих норм на звукоизоляцию в помещении поверхностная масса основных ограждающих конструкций должна составлять не менее 250-300 кг.

Звукоизолирующие ограждения - это стены, перекрытия, перегородки, окна, двери, имеющие по периметру контакты с другими ограждениями. Величина звукоизоляции однослойного ограждения характеризуется сложной нелинейной зависимостью как от частоты fзв колебания акустической волны, так и от большой группы характеристик ограждения. В общем случае эту зависимость можно представить в виде следующей функции:

R=F(fзв, m, h/fог, ρ, v),

где m - поверхностная масса ограждения;

h - коэффициент потерь энергии в материале;

fог - собственная частота колебаний ограждения;

ρ - удельная плотность материала ограждения;

v скорость звука в материале ограждения.

Одним из наиболее слабых звукоизолирующих элементов ограждающих конструкций выделенных помещений являются двери и окна. Двери имеют существенно меньшие по сравнению с основными ограждающими конструкциями поверхностные плотности, а также зазоры и щели. Стандартные двери не удовлетворяют требованиям по защите информации в помещениях от подслушивания.

Для защиты информации необходимо применять либо специально разработанные звукоизолирующие двери, либо двойные двери с тамбуром. При этом целесообразно применять утяжеленные полотна дверей, обивать их материалами со слоями ваты или войлока, использовать дополнительные уплотнительные прокладки, герметизирующие наплавы, валики и т.п. При организации тамбуров дверей звукоизоляцию повышает уплотнение щелей над полом при отсутствии порогов, а также целесообразна облицовка внутренних поверхностей тамбура звукопоглощающими покрытиями.

Окна, занимающие по условиям обеспечения освещенности достаточно большие площади ограждающих конструкций помещений, также как и двери, являются элементом

среды распространения потенциальных каналов утечки информации.

Необходимо отметить, что увеличение числа стекол не всегда приводит к увеличению звукоизоляции в диапазоне частот речевого сигнала вследствие резонансных явлений в воздушных промежутках и эффекта волнового совпадения. Разработаны конструкции окон с повышенным звукопоглощением на основе стеклопакетов с герметизацией воздушного промежутка, с заполнением при пониженном давлении промежутка между стеклами различными газовыми смесями или созданием между ними вакуума. Звукоизоляция до 5 дБ попытается при облицовке межстекольного пространства по периметру звукопоглощающим покрытием.

Следует иметь ввиду, что в общем случае звукоизоляция ограждающей конструкции, содержащей несколько элементов, должна оцениваться звукоизоляцией наиболее слабого элемента. Такими элементами чаще бывают однослойные плоские ограждения. Для повышения величины ослабления на плоское ограждение наносят слой звукопоглощающего материала, которое увеличивает звукоизоляцию R за счет дополнительного ослабления звука в звукопоглощающем материале и повышения общей массы составного ограждения.

Для повышения звукоизоляции применяют также многослойные ограждения, чаще двойные. Они состоят из двух однослойных поверхностей, разделенных в простейшем случае воздушным слоем. Между поверхностями, соединенных ребрами жесткости, помещают различные звукопоглощающие материалы. Уровень акустического сигнала Rвн в дБ за ограждением можно приближенно оценить по формуле:

$$R_{вн} \approx R_{рс} + \lg S_{ог} - R_{ог}$$

где Rрс - уровень речевого сигнала в контролируемом помещении, дБ;

Rог - звукоизолирующая способность ограждения дБ;

Sог - площадь ограждения, м2.

Для снижения опасного акустического сигнала в помещениях применяют также акустические экраны, размещаемые на пути распространения звука. Акустические экраны устанавливают между наиболее слабыми местами по звукопоглощающей способности ограждающей конструкции и расчетными точками помещения, в которых речевой сигнал должен быть неразборчив. Действие акустических экранов основано на отражении звуковых волн и образовании за экраном звуковых теней. В результате дифракции эффективность экрана повышается с увеличением соотношения размеров экрана и длины акустической волны. Размеры эффективных экранов превышают более чем в 2-3 раза длину волны. Реально достигаемая эффективность акустических экранов, покрытых звукопоглощающими материалами, составляет 8-10 дБ.

Наиболее удобны передвижные, складные и легко монтируемые акустические экраны. Акустические экраны могут использоваться для дополнительной защиты дверей, окон, технологических проемов, панелей кондиционеров, отверстий воздушной вентиляции и других элементов ограждающих конструкций, имеющих не удовлетворяющую действующим нормам локальную звукоизоляцию. Применение акустических экранов целесообразно также для защиты акустической информации в помещениях временного использования, когда их акустическая обработка нецелесообразна.

Для звукоизоляции по всем направлениям в ограниченном пространстве применяют кабины (для людей) и кожуха (для излучающих звуки механизмов и машин). Основное отличие звукоизолирующего кожуха от кабины заключается в необходимости обеспечения в кабине условий для пребывания в ней человека - вентиляции воздуха, освещения, средств связи.

В конструктивном отношении звукоизолирующие кабины делятся на каркасные и бескаркасные. В первом случае на металлическом каркасе крепятся звукопоглощающие панели. Примером таких кабин являются кабины междугородной телефонной связи.

Кабина с двухслойными звукопоглощающими плитами обеспечивает ослабление звука до 35-40 дБ. Более высокой акустическом эффективностью обладают кабины бескаркасного типа. Они собираются из готовых многослойных щитов, соединенных между собой через звукоизолирующие упругие прокладки. Такие кабины дорогие в изготовлении, но снижение уровня звука в них может достигать 50-55 дБ. Для повышения звукоизоляции минимизируют возможное число стыковочных соединений отдельных панелей между собой и с каркасом кабины, стыки тщательно герметизируют и уплотняют, применяют звукопоглощающие облицовки стен и потолка, глушат звуки средств вентиляции и кондиционирования воздуха.

Перспективными кабинами являются прозрачные переговорные кабины. Двухслойные ограждающие поверхности и стыковочные узлы этих кабин, а так/ко мебель (столик и стулья) изготавливают из органического стекла. Прозрачность ограждений и мебели позволяет быстро обнаруживать закладные устройства и контролировать во время переговоров пространство вокруг кабины. Например, кабина Л-44 и различные модификации кабины Л-45 предназначены для 2-8 человек, имеют площадь внутри кабины 4-8 м2, обеспечивают звукоизоляцию в диапазоне 300-5000 Гц не менее 25 дБ. В дальнейшем предполагается нанесение на поверхность кабины прозрачных композитивных пленок на лавсановой основе, что обеспечит одностороннюю (из кабины) проводимость света, почти в 20 раз увеличит механическую прочность прозрачных ограждающих конструкций, вдвое повысит устойчивость поверхности огню, исключит возможность лазерного подслушивания.

Звукоизолирующие кабины в зависимости от требований к изоляции звука подразделяются на 4 класса. Кабины 1-го класса должны обеспечивать ослабление звука в диапазоне 63-8000 Гц на 25-50 дБ, 2-го класса на 15-49 дБ в том же диапазоне, 3-го и 4-го классов - до 39 и 29 дБ соответственно. Наименьшие значения соответствуют низким частотам, наибольшее ослабление происходит на частотах 2000-4000 Гц.

'Звукоизолирующие кожуха проще по конструкции и изготовляются из листовых материалов (стали, дюралюминия и др.). Поверхность стенок кожу-хон облицовываются звукопоглощающими материалами толщиной 30-50 мм в виде матов из минеральной ваты, супертонкого стекла или базальтового волокна.

Кожух для блокирования передачи структурного звука устанавливается на виброизолирующих прокладках. Внутри кожуха помещаются источники звука. Кожуха бывают съемными, раздвижными и капотного типа, сплошной герметичной или неоднородной конструкции - со смотровыми окнами, открывающими дверцами, проемами для ввода коммуникаций, циркуляции воздуха. Кожуха снижают уровень звука на 20-40 дБ.

Глушение звука достигается путем интенсивного поглощения энергии акустической волны при распространении ее в специальной конструкции, называемой глушителем. Например, в момент выхода газов из цилиндра двигателя автомобиля в выходном коллекторе создается акустическая волна большой интенсивности. Она направляется по трубе в глушитель, в котором проходя через многочисленные преграды, теряет энергию и выходит из выхлопной трубы с энергией, сравнимой с энергией акустического фона. При прогорании глушителя или его съеме, что делают иногда на спортивных автомобилях для повышения их мощности, работа двигателя сопровождается интенсивным шумом. В зависимости от способа глушения звука глушители под-разделяются на абсорбционные, реактивные и комбинированные.

В абсорбционных глушителях происходит звукопоглощение в материалах и конструкции, в реактивных - в результате отражения звука обратно к источнику. Комбинированные глушители объединяют оба эти способа.

Звукопоглощение обеспечивается путем преобразования в звукопоглощающем материале кинетической энергии акустической волны в тепловую энергию. Звукопоглощающие свойства материалов оцениваются коэффициентом звукопоглощения,

определяемым отношением энергии, поглощенной в материале звуковых волн к звуковой энергии, падающей на поверхность материала.

Применение звукопоглощающих материалов при защите акустической информации имеет некоторые особенности по сравнению со звукоизоляцией. Одной из особенностей является необходимость создания непосредственно в помещении акустических условий для обеспечения разборчивости речи в различных его зонах. Таким условием является, прежде всего, обеспечение оптимального соотношения прямого и отраженного от ограждений акустических сигналов. Чрезмерное звукопоглощение приводит к ухудшению уровня сигнала в различных точках помещения, малое - к большому времени и ухудшению разборчивости речи в результате наложения различных звуков.

Обеспечение рациональных значений рассмотренных условий определяется как общим количеством звукопоглощающих материалов в помещении, так и распределением звукопоглощающих материалов по ограждающим конструкциям с учетом конфигурации и геометрических размеров помещения.

Неконструктивным свойствам различают рыхлые акустические материалы, плитные материалы, акустическая штукатурка и резонансные поглотители в виде панелей и щитов из дерева и других материалов. Средства поглощения звука в помещениях, используемые для акустической обработки помещений, подразделяют на:

- звукопоглощающие облицовки в виде акустических плит мелкой зернистой или ячеечной структуры (плиты минераловатные «Акмигран», «Акмант», «Силакпор», «Винипор», ПА/С, ПА/О, ПП-80, ППМ, ПММ);
- звукопоглощающие облицовки из слоя пористо-волокнистого материала (стеклянного или базальтового волокна, минеральной ваты) в защитной оболочке из ткани или пленки с перфорированным покрытием (металлическим, гипсовым и др.). В качестве защитных покрытий применяются: ткани марок ЭЗ-100, А-1, ТСД, пленки типа ПЭТФ, алюминиевые перфорированные панели типа ПА, ЛАП, ЛАК, листы стальные перфорированные, асбоцементные перфорированные листы, листы гипсовые типа АГП, АГШБ и др.

Плоский слой звукопоглощающего материала облицовок устанавливается на жестком основании, который крепится непосредственно или с воздушным промежутком на поверхности ограждения, к потолку или стенам.

Для дополнительного звукопоглощения и уменьшения числа переотражений от ограждений с целью снижения времени реверберации используются штучные звукопоглотители. Они представляют собой одно или многослойные объемные звукопоглощающие конструкции (в виде куба, параллелепипеда, конуса), подвешиваемые к потолку помещения. Размеры граней штучных звукопоглотителей составляют 40-400 см.

Каналы вентиляции и систем кондиционирования могут способствовать утечке информации из помещения. Передача звука через вентиляционный канал происходит по воздуху, находящемуся в полости канала, и по элементам конструкции канала. Наиболее эффективной мерой предотвращения утечки информации через воздухопроводы является установка в них абсорбционныхглушителей.

Громкость звука, воспринимаемого человеком, зависит не только от его собственной интенсивности, но и от других звуков, действующих одновременно на барабанную перепонку уха. В силу психофизиологических особенностей восприятия звука человеком интенсивность маскирующих звуков обладает асимметричностью. Она проявляется в том, что маскирующий звук оказывает относительно небольшое влияние на тоны маскируемого звука ниже его собственной частоты, но сильно затрудняет восприятие более высоких звуков. Поэтому для маскировки акустических сигналов эффективны низкочастотные акустические шумовые сигналы.

Следует отметить, что акустическое зашумление помещения обеспечивает эффективную защиту информации в нем, если акустический генератор расположен к акустическому приемнику злоумышленника ближе, чем источник информации. Например,

когда подслушивание возможно через дверь или открытое окно, то акустический генератор целесообразно разместить возле двери или на подоконнике окна. Если местонахождение акустического приемника злоумышленника неизвестно, например, закладного устройства, то размещение акустического генератора между говорящими людьми, как рекомендуют некоторые фирмы, не гарантирует надежную защиту информации. Кроме того, повышение уровня шума вынуждает собеседников к более громкой речи, что создает дискомфорт и снижает эффект от зашумления.

Более эффективным и активным универсальным способом защиты информации, передаваемым структурным звуком, является вибрационное зашумление. Шум в звуковом диапазоне в твердых телах создают пьезокерамические вибраторы акустического генератора, прикрепляемые (приклеиваемые) к поверхности зашумляемого ограждения (окна, стены, потолка и др.) или твердотельного звукопровода (батареи отопления, трубы и др.). Так как уровень структурного шума, создаваемого генератором, выше уровня речевого сигнала в твердых телах, но ниже уровня слышимости, то вибрационное зашумление целесообразно применять во всех случаях, когда существует возможность утечки с помощью структурного звука. Один виброизлучатель (вибратор) обеспечивает эффективное зашумление в радиусе 1.5-5 м.

Пассивное энергетическое скрытие акустической информации от подслушивания лазерным микрофоном заключается в ослаблении энергии акустической волны, воздействующей на оконное стекло. Оно достигается использованием штор и жалюзей, а также двойных оконных рам. Активные способы энергетического скрытия акустической информации предусматривают применение генераторов шумов в акустическом диапазоне, датчики которых приклеиваются к стеклу и вызывают его колебание по случайному закону с амплитудой, превышающей амплитуду колебаний стекла от акустической волны.

3 Способы и средства предотвращения утечки информации с помощью закладных устройств

Обнаружение закладных устройств, также как и любых других объектов, производится по их демаскирующим признакам. Чем больше демаскирующих признаков в признаковой структуре и чем они информативнее, тем выше вероятность обнаружения объекта. Каждый вид закладных устройств имеет свою признаковую структуру, позволяющую с той или иной вероятностью обнаружить закладку. Распознавание закладки, т. е. определение ее вида, назначения и характеристик, проводится в результате анализа схемотехнических и конструктивных решений. Однако внешний вид закладки и способы ее оперативного применения позволяют приблизительно определить принадлежность злоумышленника к зарубежной разведке, конкуренту или криминальным элементам.

Спецслужбы используют наиболее совершенные средства добывания, как привило, отсутствующие на рынке, и тщательно готовят операцию по установке закладок. Криминальные элементы пользуются средствами, имеющимися на рынке, и действуют более грубо. Разведка коммерческих структур применяет закладки промышленного изготовления и тщательно скрывает от конкурента свои намерения получения конфиденциальной информации нелегальными способами.

Наиболее информативными признаками микрофонной закладки являются:

- тонкий провод, проложенный от малогабаритного микрофона закладки в другое помещение;
- наличие в кожухе закладки одного или нескольких отверстий.

Признаковые структуры некамуфлированнойрадиозакладки включают:

- радиоизлучения с модуляцией радиосигнала акустическим сигналом, циркулирующим в помещении;

- признаки внешнего вида - малогабаритный предмет непонятного назначения в форме параллелепипеда, цилиндра без или с одним органом управления (выключателем питания) на поверхности;
- одно или несколько отверстий малого диаметра в кожухе;
- наличие, но не всегда, небольшого отрезка провода, выходящего из кожуха;
- присутствие полупроводниковых элементов, выявляемых при облучении обследуемых предметов нелинейными радиолокаторами;
- наличие в устройстве металлических проводников или других деталей, определяемых металлодетекторами или при просвечивании предмета рентгеновскими лучами.

Камуфлированные радиозакладки по внешнему виду на первый взгляд не отличаются от объекта имитации, особенно если закладка устанавливается в корпус бытового предмета без изменения его внешнего вида. Некоторые камуфлированные закладные устройства неотличимы от оригиналов при внешнем осмотре. Например, на поверхность закладки-конденсатора наносятся заводские реквизиты - тип, величина емкости, номер серии и т. д. Назначение таких закладок можно выявить путем разборки или просвечивания их рентгеновскими лучами.

Однако следует иметь ввиду, что закладки, камуфлированные под малогабаритные предметы, снижают функциональные возможности этих предметов. Поэтому обнаруженные ограничения функций средств оргтехники, электробытовых устройств и др. могут служить косвенными признаками установки в них закладных устройств. Например, в шариковой авторучке закладное устройство занимает приблизительно половину ее длины, в результате чего резко укорачивается пишущий стержень и сокращается время нормальной работы ручки. Кроме того, такую ручку нельзя разобрать, например, для замены стержня, так как разбираемые части склеивают.

Не могут применяться по прямому назначению электролампочки типа РК-520 с установленной в цоколь закладкой. Однако другой тип электролампочки — РК-560-S лишен этого признака. Визуально выявить наличие в этой электролампе радиозакладки невозможно.

Вследствие постоянной конкуренции между производителями закладных устройств и средств их обнаружения и локализации на рынке существует множество видов и типов технических средств как тех, так и других. Классификация технических средств обнаружения и локализации закладных устройств приведена на рис.4.7.

Средства радиоконтроля помещения предназначены для обнаружения закладных устройств, излучающих радиоволны во время их поиска. Для обнаружения неизлучающих при поиске закладок - дистанционно управляемых и передающих сигналы по проводам, применяются средства, реагирующие не на радиоизлучения, а на иные демаскирующие признаки закладок. Наконец, средства подавления закладных устройств обеспечивают энергетическое скрытие их сигналов, нарушение работоспособности закладок или их физическое разрушение.

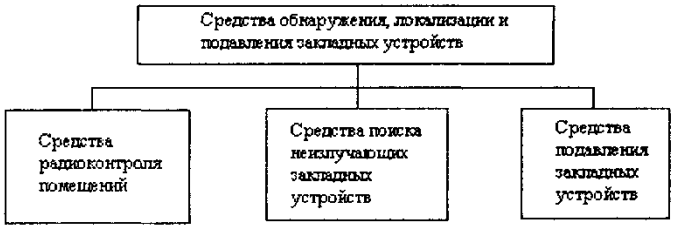


Рис. 4.7 - Классификация средств обнаружения и локализации закладных устройств

Учитывая, что радиоизлучающие закладки преобладают на рынке закладных устройств, существуют разнообразные средства радиоконтроля обследуемых помещений:

от простейших индикаторов электромагнитного поля до сложных автоматизированных комплексов. Классификация обнаружителей радиоизлучений закладных устройств указана на рис. 4.8.

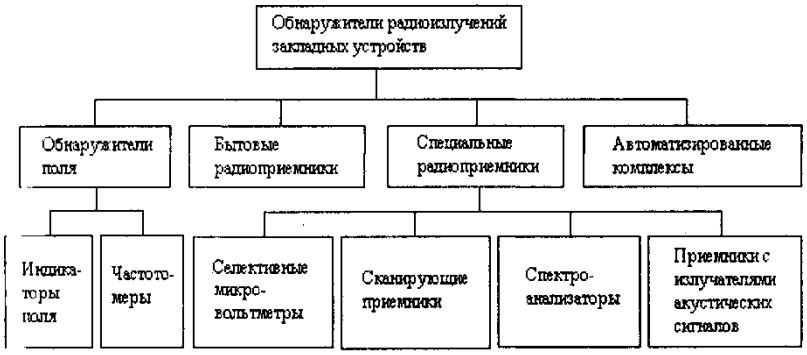


Рис.4.8 - Классификация средств обнаружения излучений закладных устройств

Простейшими и наиболее дешевыми обнаружителями радиоизлучений складных устройств являются индикаторы электромагнитных полей. Наиболее простые из них - обнаружители поля, которые световым или звуковым сигналом информируют оператора о наличии в месте расположения антенны индикатора электромагнитного поля с напряженностью выше фоновой. Более сложные из них - частотомеры обеспечивают, кроме того, измерение частоты колебаний поля. Но чувствительность обнаружителей поля мала, поэтому с их помощью можно обнаруживать поля радиозакладок в непосредственной близости от источника излучения.

Существенно большую чувствительность имеют супергетеродинные бытовые приемники. Однако возможности использования бытовых радиоприемников для поиска радиозакладок ограничены радиовещательным диапазоном и видами модуляции, применяемыми в радиовещании (АМ и ЧМ). С помощью преобразователей (конверторов) можно перестроить частотный диапазон бытового радиоприемника на частоту радиозакладки, если она известна. Но для поиска радиозакладных устройств с неизвестной частотой перестроенные бытовые радиоприемники неэффективны, так как они обеспечивают поиск частоты закладки в узком диапазоне частот.

Широкими возможностями по обнаружению радиозакладок обладают специальные приемники. Среди них все большую популярность приобретают радиоприемники с автоматизированным сканированием радиодиапазона. Они обеспечивают поиск в диапазоне частот, перекрывающем частоты почти всех применяемых радиозакладок - от долей МГц до единиц ГГц. Кроме того, сканирующие радиоприемники имеют, как правило, оперативную память для запоминания частот не представляющих интерес источников излучения, прежде всего, радиовещательных и служебных радиостанций.

Информационно-техническое сопряжение сканирующих приемников с переносными компьютерами послужило технической основой для создания автоматизированных комплексов для быстрого и надежного поиска радиоизлучающих подслушивающих устройств.

Но дистанционно управляемые радиозакладки и закладки, передающие информацию по проводам, не обнаруживаются аппаратурой радио контроля. Для их поиска используются демаскирующие признаки материала конструкции и элементов схемы закладного устройства, а также признаки сигналов, распространяющихся по проводам. С целью обнаружения и локализации таких закладок применяются или создаются специальные технические средства, классификация которых приведена на рис.

4.9.

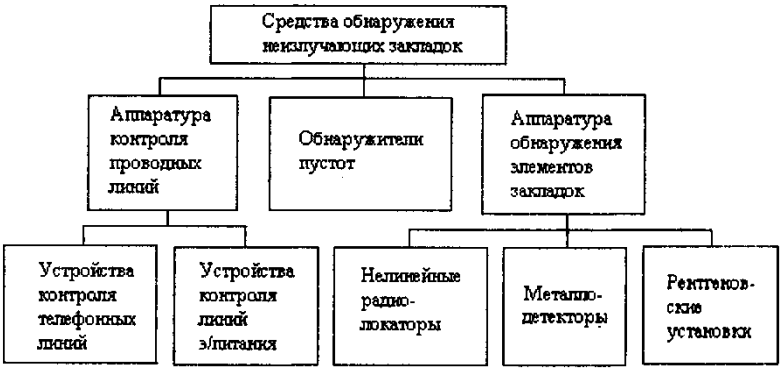


Рис. 4.9 - Классификация средств обнаружения неизлучающих закладок

Аппаратура для контроля проводных линий предназначена для выявления в них опасных сигналов и их источников, в том числе закладных устройств. Так как основными направляющими линиями, по которым передаются от закладных устройств электрические сигналы с информацией, являются телефонные линии и цепи электропитания, то соответствующие средства контроля включают приборы контроля телефонных линий и линий электропитания.

Обнаружители пустот позволяют обнаруживать возможные места установки закладных устройств в пустотах стен или других деревянных или кирпичных конструкциях.

Большую группу образуют средства обнаружения или локализации закладных устройств по физическим свойствам элементов электрической схемы или конструкции. Такими элементами являются: полупроводниковые приборы, которые применяются в любых закладных устройствах, металлические детали конструкции, элементы, поглощающие рентгеновские лучи.

Из этих средств наиболее достоверные результаты обеспечивают средства для обнаружения полупроводниковых элементов по их нелинейным свойствам - нелинейные радиолокаторы. Принципы работы нелинейных радиолокаторов близки к принципам работы радиолокационных станций, широко применяемых для радиолокационного наблюдения различных объектов. Существенное отличие заключается в том, что если приемник радиолокационной станции принимает отраженный от объекта эхо-сигнал на частоте излучаемого сигнала, то приемник нелинейного локатора принимает 2-ю и 3-ю гармоники отраженного сигнала. Появление в отраженном сигнале этих гармоник обусловлено нелинейностью характеристик выход/вход полу проводников. В результате нелинейного преобразования электрического сигнала, индуцируемого в элементах схемы закладного устройства высокочастотным полем локатора, образуется сигнал, в спектре которого присутствуют кроме основной частоты ее гармоники. Количество и амплитуда гармоник зависят от характера нелинейности и мощности электромагнитного поля.

Металлодетекторы (металлоискатели) реагируют на наличие в зоне поиска электропроводных материалов, прежде всего, металлов, и позволяют обнаруживать корпуса или другие металлические элементы закладки.

Переносные рентгеновские установки применяются для просвечивания предметов, назначение которых не удается выявить без их разборки, прежде всего, тогда, когда разборка невозможна без разрушения найденного предмета.

3. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ПРОВЕДЕНИЮ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

3.1 Практическое занятие № 1 (2 часа).

Тема: «Выбор объекта и определение информационных ресурсов**»**

3.1.1 Задание для работы:

1. Выбрать критически важный объект
2. Определить используемые им информационные ресурсы

3.1.2 Краткое описание проводимого занятия:

В процессе занятия необходимо выбрать для рассмотрения объект, отнесённый к классу критически важных. Определить на объекте организационную структуру и используемые на объекте информационные ресурсы.

3.1.3 Результаты и выводы:

Сделать вывод о проделанной работе, какие ресурсы и для чего используются. Определить степень важности их защиты.

3.2 Практическое занятие № 2-3 (4 часа).

Тема: «Разработка технического паспорта объекта**»**

3.2.1 Задание для работы:

1. Определить что такое технический паспорт.
2. Определить какая информация заносится в технический паспорт объекта.
3. Составить технический паспорт для выбранного объекта КВО

3.2.2 Краткое описание проводимого занятия:

В процессе занятия необходимо изучить термин технический паспорт, определить от чего зависит характер информации, включаемой в технический паспорт.Определить нормативно-правовые акты, согласно которым составление паспорта является обязательной процедурой. Составить примерный технический паспорт для выбранного объекта КВО.

3.2.3 Результаты и выводы:

Сделать выводы о проделанной работе. Предоставить паспорт объекта КВО.

3.3 Практическое занятие № 4 (2 часа).

Тема: «Моделирование каналов утечки информации**»**

3.3.1 Задание для работы:

1. Определить существующие виды каналов утечки информации.
2. Определить возможные каналы утечки информации на выбранном объекте КВО

3.3.2 Краткое описание проводимого занятия:

Изучить источники по существующим видам каналов утечки информации. Определить все возможные каналы утечки информации на выбранном объекте КВО. Провести анализ каналов и составить таблицу.

3.3.3 Результаты и выводы:

Сделать выводы о проделанной работе. Предоставить таблицу каналов утечки информации.

3.1 Практическое занятие № 5 (2 часа).

Тема: «Разработка модели нарушителя технических каналов утечки информации для объекта защиты.**»**

3.4.1 Задание для работы:

1. Ознакомиться с нормативно-правовыми актами ФСТЭК и ФСБ по моделям нарушителя.

2. Определить модель нарушителя для выбранного объекта КВО.

3.4.2 Краткое описание проводимого занятия:

В процессе проводимого занятия необходимо изучить нормативно-правовые акты ФСТЭК и ФСБ по модели нарушителя информационной безопасности по техническим каналам утечки. В соответствии с изученными документами составить модель нарушителя для выбранного объекта КВО.

3.4.3 Результаты и выводы:

Сделать выводы о проделанной работе. Предоставить модель нарушителя

3.5 Практическое занятие № 6 (2 часа).

Тема: «Разработка модели угроз технических каналов утечки информации для объекта защиты**»**

3.5.1 Задание для работы:

1. Ознакомиться с нормативно-правовыми актами ФСТЭК и ФСБ по моделям угроз.

2. Определить модель угроз для выбранного объекта КВО.

3.5.2 Краткое описание проводимого занятия:

В процессе проводимого занятия необходимо изучить нормативно-правовые акты ФСТЭК и ФСБ по модели угроз информационной безопасности по техническим каналам утечки. В соответствии с изученными документами составить модель угроз для выбранного объекта КВО.

3.5.3 Результаты и выводы:

Сделать выводы о проделанной работе. Предоставить модель угроз технических каналов утечки информации.

3.6 Практическое занятие № 7-8 - (4 часа).

Тема: «Разработка рекомендаций по выбору и установке технических средств защиты информации на критически важном объекте**»**

3.6.1 Задание для работы:

1. Ознакомиться с нормативно-правовыми актами ФСТЭК и ФСБ

2. Разработать рекомендации по выбору и установке технических средств защиты информации на выбранном критически важном объекте

3.6.2 Краткое описание проводимого занятия:

В процессе проводимого занятия необходимо изучить нормативно-правовые акты ФСТЭК и ФСБ. Разработать рекомендации по выбору и установке технических средств защиты информации на выбранном критически важном объекте

3.6.3 Результаты и выводы:

Сделать выводы о проделанной работе. Предоставить рекомендации по выбору и установке технических средств защиты информации на выбранном КВО.