**1.Техническая защита информации. Основные термины и определения.**

техническая защита информации; ТЗИ: Деятельность, направленная на обеспечение некриптографическими методами безопасности информации (данных), подлежащей защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств

угроза (безопасности информации): Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации

источник угрозы безопасности информации: Субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации

уязвимость (информационной системы); брешь: Свойство информационной системы, предоставляющее возможность реализации угроз безопасности обрабатываемой в ней информации.

утечка (информации) по техническому каналу: Неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации

перехват (информации): Неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов

несанкционированный доступ к информации [ресурсам информационной системы]; НСД: Доступ к информации [ресурсам информационной системы], осуществляемый с нарушением установленных прав и (или) правил доступа к информации [ресурсам информационной системы] с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

несанкционированное воздействие на информацию [ресурсы информационной системы]; НСВ: Изменение, уничтожение или копирование информации [ресурсов информационной системы], осуществляемое с нарушением установленных прав и (или) правил.

компьютерная атака: целенаправленное несанкционированное воздействие на информацию, на ресурс информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств

сетевая атака: компьютерная атака с использованием протоколов межсетевого взаимодействия

несанкционированное блокирование доступа к информации [ресурсам информационной системы]; отказ в обслуживании: Создание условий, препятствующих доступу к информации [ресурсам информационной системы] субъекту, имеющему право на него.

закладочное устройство; закладка: Элемент средства съема информации или воздействия на нее, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации.

вредоносная программа: Программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информацию или ресурсы информационной системы

(компьютерный) вирус: Исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения.

недекларированные возможности (программного обеспечения): Функциональные возможности программного обеспечения, не описанные в документации

программная закладка: Скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие

защищаемый объект информатизации: Объект информатизации, предназначенный для обработки защищаемой информации с требуемым уровнем ее защищенности

защищаемая информационная система: Информационная система, предназначенная для обработки защищаемой информации с требуемым уровнем ее защищенности

защищаемые ресурсы (информационной системы): Ресурсы, использующиеся в информационной системе при обработке защищаемой информации с требуемым уровнем ее защищенности

защищаемая информационная технология: Информационная технология, предназначенная для сбора, хранения, обработки, передачи и использования защищаемой информации с требуемым уровнем ее защищенности

защищаемые программные средства: Программные средства, используемые в информационной системе при обработке защищаемой информации с требуемым уровнем ее защищенности

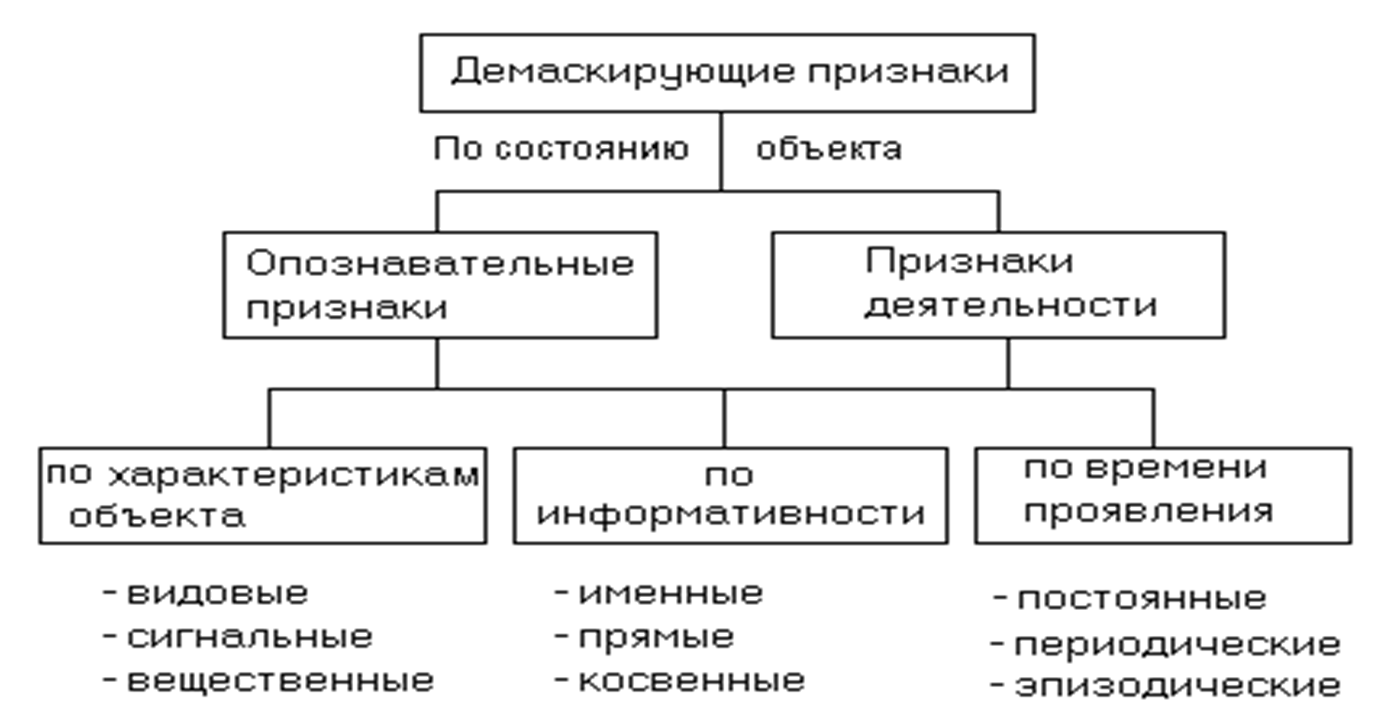
защищаемая сеть связи: Сеть связи, используемая при обмене защищаемой информацией с требуемым уровнем ее защищенности

техника защиты информации: Средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ Р 50.1.056-2005 Техническая защита информации. Основные термины и определения

**2. Демаскирующие признаки объектов.**

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

Ik = (N - Nk) / N,

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

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.

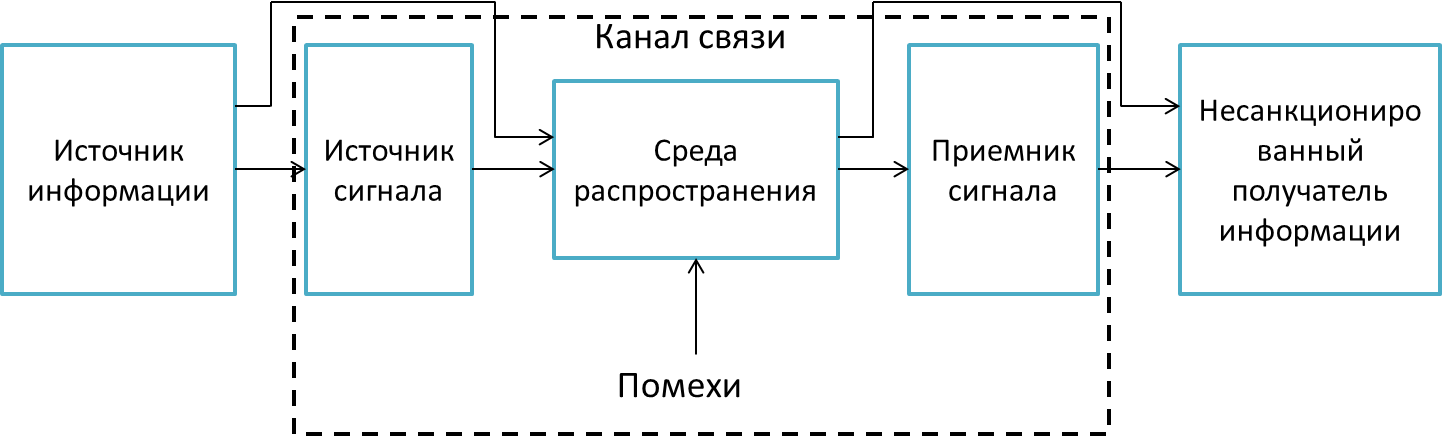
Таким образом, совокупность демаскирующих признаков рассмотренных трех групп представляет модель объекта, описывающую его внешний вид, излучаемые им поля, внутреннюю структуру и химический состав содержащихся в нем веществ.

**3. Виды и структура технических каналов утечки информации**

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.



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.



**4. Характеристики 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:

 С=Flog2 (1+Pс/Pп),

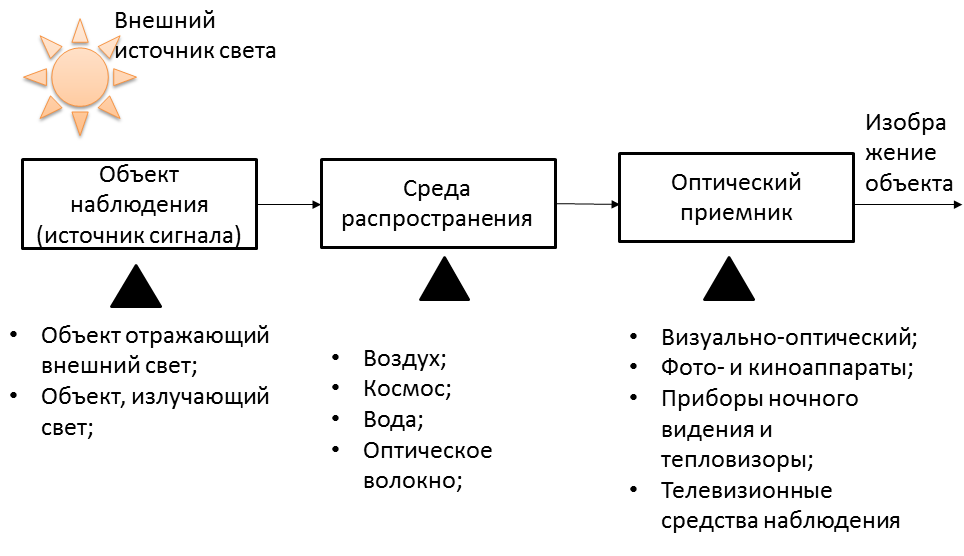
где F-ширина полосы пропускания канала связи;

Pс и Pп - мощность сигнала и помехи (в виде белого шума) в полосе пропускания канала соответственно.

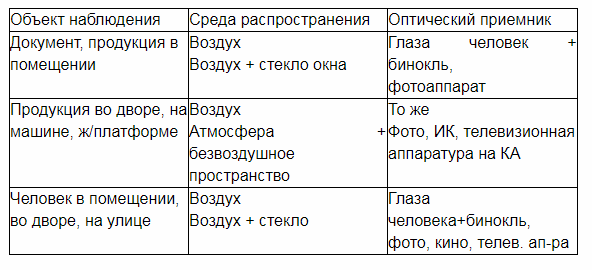
Следовательно, пропускная способность канала связи является интегральной характеристикой, учитывающей как ширину полос частот сигнала, которую пропускает канал, так и его энергетику.

Чем меньше отношение мощностей сигнала и помехи, тем больше ошибок в принятом сообщении и тем меньше количество переданной информации.

**5. Структура оптического канала утечки информации**



**6. Классификация оптических каналов утечки информации.**



**7. 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.

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 а = arcsin(nж/no),

где nж; no — 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.

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.

**8. 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.

**9. Средства добывания информации в оптическом диапазоне волн.**

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. Ее можно представить в виде, приведенном на рис.



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.

**10. 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.

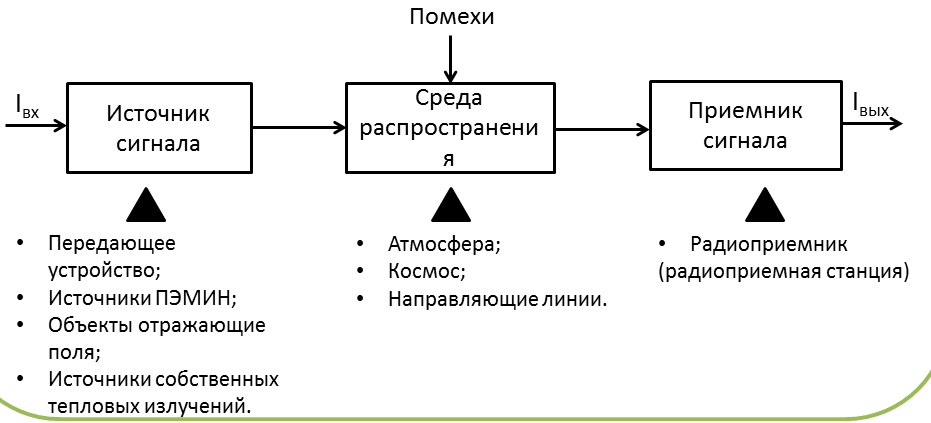
В радиоэлектронном канале производится перехват радио- и электрических сигналов, а также радиолокационное и радиотеплолокационное наблюдение.

Следовательно, в рамках этого кана­ла утечки добывается семантическая информация, видовые и сиг­нальные демаскирующие признаки.

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

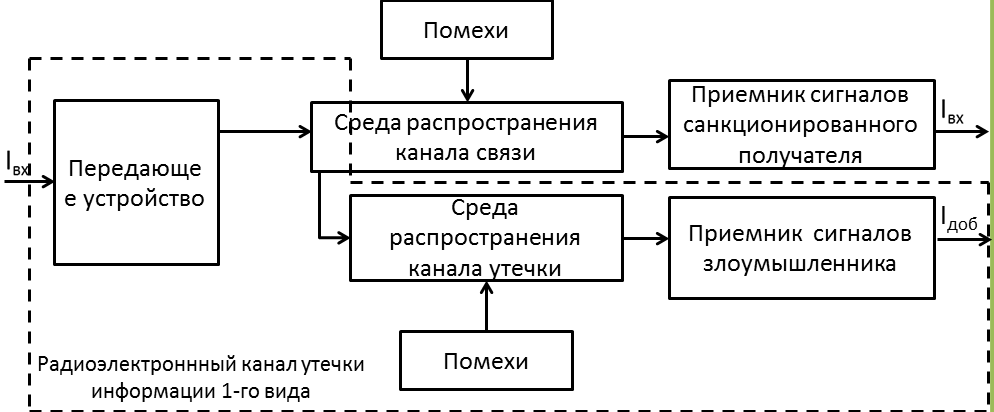
**11. Виды и структура радиоэлектронных каналов утечки информации.**

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



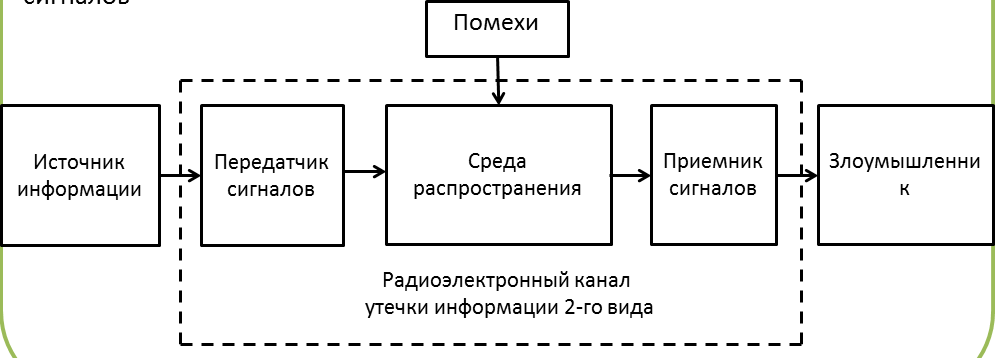
Радиоэлектронные каналы в зависимости от вида источни­ков сигналов можно разделить на каналы 1 и 2-го вида. В каналах утечки первого вида производится перехват информации, переда­ваемой по функциональному каналу связи.

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 проводного функционального 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.

**12. Радиоэлектронные каналы 1-го вида.**

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.

Среда распространения канала связи

Передающее устройство

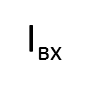
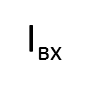
Помехи

Среда распространения канала утечки

Приемник сигналов санкционированного получателя

Приемник сигналов злоумышленника

Помехи



Iдоб

Радиоэлектроннный канал утечки информации 1-го вида

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 проводного функционального 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.

**13. Радиоэлектронные каналы 2-го вида.**

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

Источник информации

Передатчик сигналов

Среда распространения

Приемник сигналов

Злоумышленник

Помехи

Радиоэлектронный канал

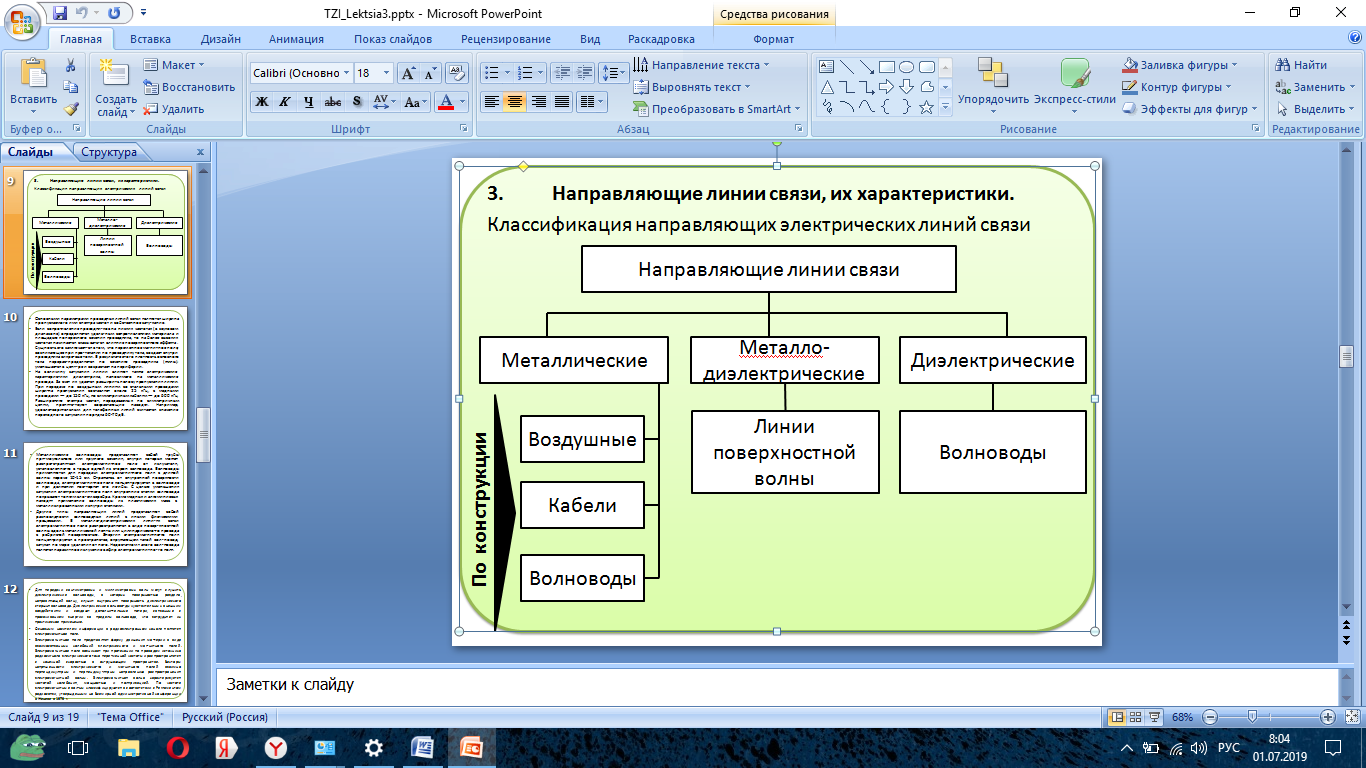
утечки информации 2-го вида

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.

**14. Направляющие линии связи, их характеристики.**

Классификация направляющих электрических линий связи



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.

**15. Средства перехвата информации, обрабатываемой средствами вычислительной техники**

Совокупность источника информативного сигнала (в данном случае - СВТ), технического средства, осуществляющего перехват информации, и физической среды, в которой распространяется информативный сигнал, называется техническим каналом утечки 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.

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

**Рисунок** - ***Схема технического канала утечки информации, обрабатываемого средствами вычислительной техники***

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.

**17. 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 (TCP ПЭМИН).

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

**18. Электрические каналы утечки информации**

Причинами возникновения электриче­ских каналов утечки информации являются наводки информативных сигналов, под кото­рыми понимаются токи и напряжения в токопроводящих элементах, вызванные побочны­ми электромагнитными излучениями, ёмкост­ными и индуктивными связями.

     Наводки информативных сигналов мо­гут возникнуть:

- в линиях электропитания ТСОИ;

- в линиях электропитания и соединитель­ных линиях ВТСС;

- в цепях заземления ТСОИ и ВТСС;

в посторонних проводниках (металличе­ских трубах систем отопления, водоснаб­жения, металлоконструкциях и т.д.).

В зависимости от причин возникнове­ния наводки информативных сигналов можно разделить на:

а) наводки информативных сигналов в электрических цепях ТСОИ, вызванные ин­формативными побочными и (или) паразитны­ми электромагнитными излучениями ТСОИ;

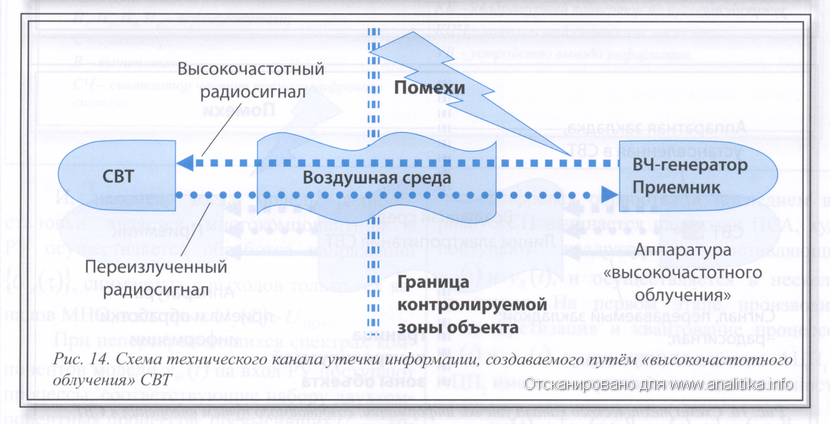
б) наводки информативных сигналов в соединительных линиях ВТСС и посторонних проводниках, вызванные информативными побочными и (или) паразитными электромаг­нитными излучениями ТСОИ;

в) наводки информативных сигналов в электрических цепях ТСОИ, вызванные вну­тренними ёмкостными и (или) индуктивны­ми связями («просачивание» информативных сигналов в цепи электропитания через блоки питания ТСОИ);

г) наводки информативных сигналов в це­пях заземления ТСОИ, вызванные информатив­ными ПЭМИ ТСОИ, а также гальванической свя­зью схемной (рабочей) земли и блоков ТСОИ.

**19. Специально создаваемые технические каналы утечки информации**

Наряду с пассивными способами перехвата информации, обрабатываемой СВТ, возможно использование и активных способов, в частности, способа «высокочастотного облучения», при котором СВТ облучается мощным вы­сокочастотным гармоническим сигналом (для этих целей используется высокочастотный ге­нератор с направленной антенной, имеющей узкую диаграмму направленности). При взаи­модействии облучающего электромагнитного поля с элементами СВТ происходит модуля­ция вторичного излучения информативным сигналом. Переизлучённый сигнал принима­ется приёмным устройством средства развед­ки и детектируется.

****

***Схема технического канала утечки информации,  создаваемого путём «высокочастотного облучения» СВТ***

Для перехвата информации, обрабаты­ваемой СВТ, возможно также использование электронных устройств перехвата информа­ции (закладных устройств), скрытно вне­дряемых в технические средства и системы.

Под ***аппаратной закладкой*** понимают электронное устройство, скрытно устанавливаемое (внедряемое) в СВТ с целью обеспечить утечку информации, нарушение ее целостности или блокирование.

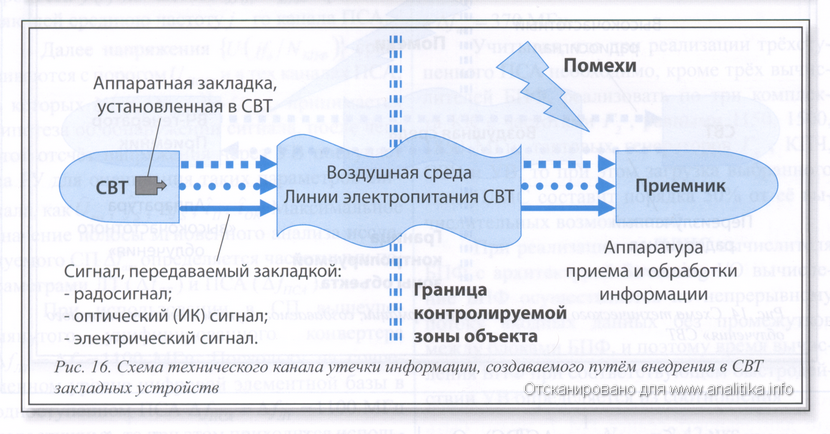
Аппаратная закладка, как правило, состоит из:

* блока перехвата;
* блока передачи информации (или модуля записи информации);
* блока ДУ (при необходимости);

блока питания.

Перехваченная с помощью закладных устройств информация или непосредствен­но передаётся по каналу связи на приёмный пункт, или записывается в специальное запо­минающее устройство и передаётся только по команде управления.

Для передачи информации на приём­ный пункт могут использоваться радиоканал, оптический (инфракрасный) канал или линии электропитания СВТ.

***Схема технического канала утечки информации,   
создаваемого путём внедрения в СВТ закладных устройств***

Закладные устройства, внедряемые в СВТ, по виду перехватываемой информации можно разделить на:

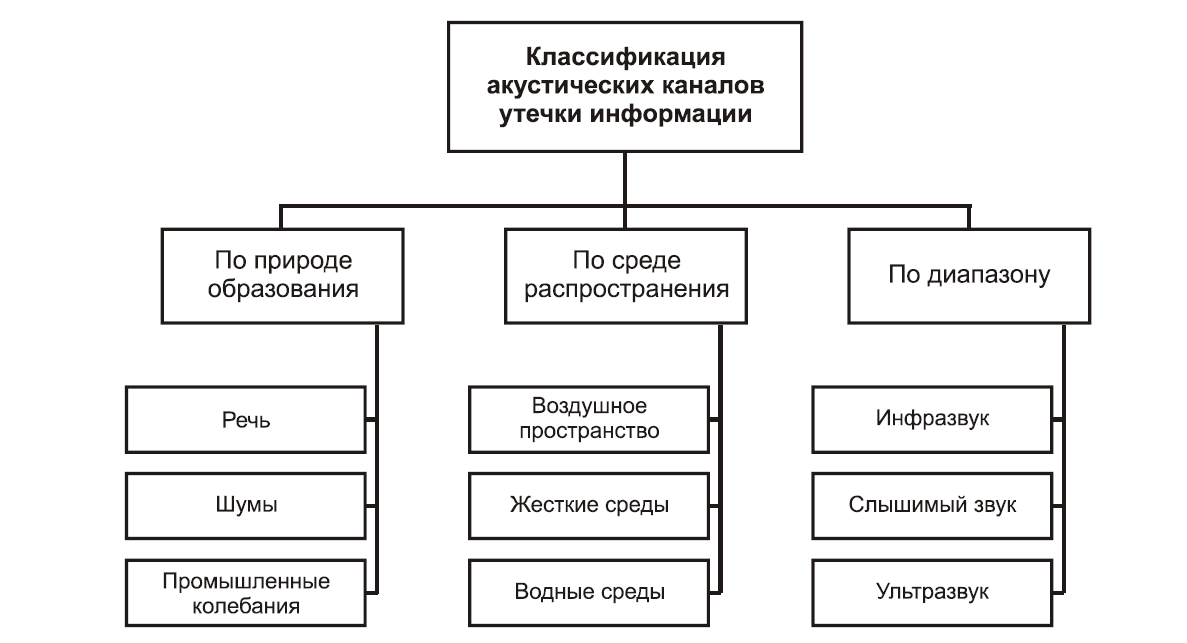
- аппаратные закладки для перехвата изобра­жений, выводимых на экран монитора;

- аппаратные закладки для перехвата инфор­мации, вводимой с клавиатуры ПЭВМ;

- аппаратные закладки для перехвата информации, выводимой на периферийные устройства (например, принтер);

* аппаратные закладки для перехвата ин­формации, записываемой на жёсткий диск ПЭВМ.

**20. Классификация акустических каналов утечки информации.**

****

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.

**21. «Заходовые» методы полученияакустической 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.

“Телефонное ухо”. 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.

**22. «Беззаходовые»методы получения акустической 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.).

Направленные акустические микрофоны (НАМ). 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.

1. **Средства добывания информации в акустическом диапазоне волн.**

Непосредственное (ушами) подслушивание ограничено малым расстоянием от источника звука - в лучшем случае около десяти метров. Малая дальность непосредственного подслушивания обусловлена не только малой мощностью акустических сигналов и большим затуханием их в среде распространения, но и тем, что уши человека имеют широкую диаграмму направленности (близкую к 180°), в силу чего на барабанную перепонку поступают практически все внешние акустические шумы.

Кроме того, шумы поднимают порог чувствительности слуховой системы человека. Но одновременно это физиологическое свойство слуховой системы человека позволяет ему адаптироваться к зашумленности среды обитания, например в жилых помещениях возле транспортных магистралей большого города.

Для непосредственного подслушивания в условиях города злоумышленнику необходимо приблизиться к источнику информации на несколько метров, что существенно ухудшает скрытность добывания информации.

Технические средства подслушивания расширяют и дополняют возможности слуховой системы человека за счет:

• приема и прослушивания акустических сигналов, распространяющихся в воде и твердых телах;

• повышения дальности подслушивания речевой информации по сравнению с непосредственным подслушиванием;

• коррекции спектра акустического сигнала, распространяющегося в среде с неравномерной амплитудно-частотной характеристикой коэффициента передачи или затухания;

• выделения акустического сигнала из смеси его и шумов;

• прослушивания речи, выделяемой из перехваченных радио- и электрических сигналов функциональных каналов связи и из сигналов побочных излучений и наводок;

• ретрансляции добываемой речевой информации на сколь угодно большое расстояние.

Конкретный способ подслушивания реализуется с использованием соответствующих технических средств. Совокупность технических средств, обеспечивающих функции добывания семантической и признаковой акустической информации, представляет собой комплекс средств подслушивания. Структурная схема типового комплекса приведена на рис. 15.1.

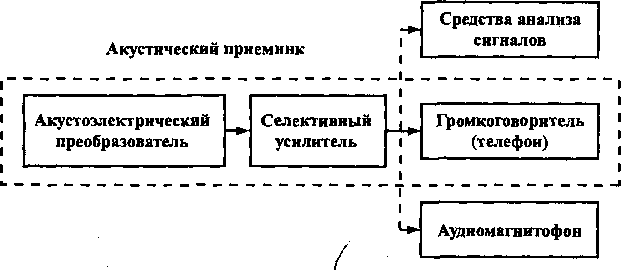


Рис. Структурная схема комплекса средств подслушивания

Основной частью комплекса является акустический приемник. Он производит селекцию по пространству и частоте акустических сигналов, распространяющихся в атмосфере, воде, твердых телах, преобразует их в электрические сигналы, усиливает и обрабатывает электрические сигналы и преобразует их в акустическую волну для обеспечения восприятия информации слуховой системой человека. Акустический приемник содержит акустоэлектри-ческий преобразователь, селективный усилитель и электроакустический преобразователь (телефон, громкоговоритель).

Акустические приемники для приема акустической волны, распространяющейся в воздухе, воде, твердой среде (в инженерных конструкциях), в грунте, отличаются видом акустоэлек-трического преобразователя. Иногда по виду акустоэлектричес-кого преобразователя называют весь акустический приемник. Акустоэлектрический преобразователь акустической волны, распространяющейся в воздухе, называется микрофоном, преобразователь волны, распространяющейся в твердой среде, - стетоскопом и акселерометром, в земной поверхности - геофоном, а в воде- гидрофоном.

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.

1. **Классификация материально-вещественных каналов утечки информации.**



1. **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.

1. **Особенности утечки информации о радиоактивных веществах.**

Утечка информации о радиоактивных веществах возможна в результате выноса радиоактивных веществ сотрудниками организации или регистрации злоумышленником их излучений с помощью соответствующих приборов. Утечка информации о радиоактивных веществах возможна по двум каналам: оптическому, носителями информации в котором являются электромагнитные поля в виде у-излучений, и вещественному, носителями информации в котором являются элементарные а- и Р-частицы.

Дальность канала утечки информации о радиоактивных веществах через их излучения невелика: для а-излучений она составляет в воздухе единицы мм, ^-излучений - см, только у-излучения можно регистрировать на удалении в сотни и более метров от источника излучения.

Добыванием информации о радиоактивных веществах занимается радиационная разведка. Демаскирующими признаками радиоактивных веществ являются ионизирующие (радиоактивные) излучения (нейтронов, гамма-лучей, альфа- и бета-частиц - п, у, а, р соответственно). Альфа-излучение (распад) представляет собой самопроизвольное превращение ядер, сопровождающееся испусканием со скоростью 14000-20000 км/с двух протонов и двух нейтронов, образующих ядро гелия. Бета-излучение представляет собой поток электронов, скорости которых близки к скорости света. Гамма-излучение является электромагнитным излучением с длиной волны менее 100 мкм. Заряд и кинетическую энергию а- и Р-частиц определяют по их отклонению в электрическом и магнитном полях известной напряженности. Энергию и длину волны у-излучения рассчитывают по энергии электронов, освобождаемых из различных веществ под действием этого излучения.

Для обнаружения и измерения радиоактивных излучений используют средства, реализующие фотографический, сцинтилля-ционный, люминесцентный, химический и ионизационный методы.

Основу фотографического метода составляет зависимость степени почернения фотоэмульсии от поглощенной энергии излучения. Под воздействием ионизирующих излучений молекулы бромистого серебра фотоэмульсии распадаются на бром и серебро. Кристаллы серебра вызывают почернение фотопленки при ее проявлении. По степени почернения определяют дозу излучения.

Наиболее широко применяются ионизационные методы обнаружения радиоактивного излучения. Структура типового прибора радиационной разведки, реализующей эти методы, приведена на рис. 18.1.

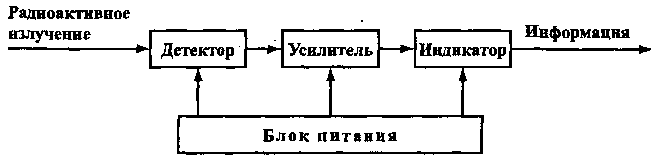


Рис. Структурная схема прибора радиационной разведки

Детектор преобразует энергию радиоактивного излучения в электрические сигналы, которые после усиления поступают на стрелочный или цифровой индикатор. В качестве детектора используются ионизационные камеры, газоразрядные счетчики, кристаллы полупроводника.

1. **Системный подход к инженерно-технической защите информации.**

Силы и средства, реализующие цели, задачи и методы инженерно-технической разведки, образуют систему инженерно-технической защиты информации. Любая сложная система имеет иерархическую структуру. Первый уровень структуры образуют подсистемы, ниже — комплексы, еще ниже — подкомплексы.

Каждый структурный элемент объединяет силы и средства, решающие определенные задачи системы. В соответствии с рассмотренными методами в состав системы должны входить подсистемы физической защиты информации и подсистема защиты информации от утечки 

1. **Сущность системного подхода и системного анализа.**

Для реализации общих принципов инженерно-технической защиты информации (надежности, непрерывности, целеустремленности, активности, гибкости, скрытности, экономичности, комплексности) в условиях изменения условий необходимо ***управление силами и средствами системы***. Учитывая, что традиционно *подсистемы физической защиты* и *защиты от утечки* курируются разными ведомствами, а пользователь информации один, то ***подсистема управления должна согласовывать деятельность сил и средств этих подсистем.***

Нормативные указания отображаются в инструкциях по обеспечению защиты информации. Но в инструкциях невозможно учесть все ситуации. Силы и средства системы должны обеспечить принятие рационального решения при возникновении нетиповых ситуаций в условиях дефицита времени.

Так как защита информации невозможна без контроля ее эффективности, то важнейшей задачей подсистемы управления является организация и проведение различных видов контроля мер по защите.

В соответствии с **системным подходом** *подсистемы физической защиты информации* и *защиты ее от утечки* при их автономном анализе рассматриваются как системы.

1. **Основные этапы проектирования системы защиты информации техническими средствами.**

Эффективность любой системы в значительной степени зависит от эффективности управления ее силами и средствами. Без управления она раньше или позже ухудшит свои показатели и потеряет работоспособность. Бытует мнение, что эффективность хорошо работающей организации не зависит от присутствия или отсутствия на рабочем месте ее руководителя. Это утверждение отчасти справедливо для стационарных условий. Однако при появлении нетиповых ситуаций без руководителя не обойтись. Поэтому управление необходимо, прежде всего, для адаптации системы к изменениям условий ее функционирования. Чем более организованной и управляемой является система, тем более продолжительное время она может противостоять многочисленным угрозам.

Органы управления любой системы на основе данных о состоянии элементов системы, а также внешних и внутренних сигналов формируют команды управления, которые через управляемые объекты (другие элементы системы) обеспечивают решение системой поставленных задач и достижение ее целей.

Внешние и внутренние воздействия на элементы системы изменяют ее состояние, определяющее, например, уровень безопасности информации. Сигнал тревоги от извещателя, например, характеризует с определенной вероятностью появление реальной угрозы защищаемой информации, Однако команды управления по ее нейтрализации могут существенно отличаться в зависимости от ситуации.

Простейшие команды управления представляют собой откли­ки на воздействия.

1. **Принципы моделирования объектов защиты и технических каналов утечки информации.**

Основу управления силами и средствами инженерно-технической защиты также составляет ее модель. Она представляет собой совокупность документов и программ, обеспечивающих Достижение заданных значений показателей эффективности системы защиты. Модель содержит руководящие и нормативно-методические документы вышестоящих органов и разрабатываемые в организации. Например, к таким документам относятся положение о подразделении (его структуре, правах и обязанностях сотрудников), непосредственно обеспечивающее защиту информации, руководство по защите информации в организации, инструкция дежурным и др.

Управление силами и средствами защиты информации достигается путем долгосрочного и кратковременного планирования инженерно-технической защиты информации, нормативного и оперативного управления силами и средствами, а также контролем действий людей и работоспособности технических средств.

**План защиты** является одним из основных элементов модели защиты. В нем на основе результатов состояния защиты и прогнозируемых угроз определяются необходимые меры по совершенствованию инженерно-технической защиты информации, сроки и должностные лица, ответственные за их реализацию.

**Нормативное управление** представляет собой постановку задач и контроль их выполнения в соответствии с планом защиты.

Однако даже в очень подробном плане невозможно учесть все ситуации, которые могут возникнуть в реальных условиях. Более того, как показывает практика управления, чрезмерная детализация плана далеко не всегда приводит к повышению эффективности работы системы, особенно в случаях, когда разработчики планов недостаточно учитывают возможные условия. Лучшие результаты достигаются путем оперативного (ситуационного) управления. При оперативном управлении решение по защите информации принимается для конкретных условий появления нештатной (нетиповой) реальной угрозы. При оперативном управлении исходные данные более точные, чем при нормативном, но возникает, как правило, дефицит времени на принятие решения по нейтрализации возникшей угрозы. Дефицит времени может вызвать у лиц, принимающих решение, например у дежурного в ночное время, стрессовое состояние и привести к грубым ошибкам.

Необходимым условием эффективного управления является контроль выполнения плана и команд управления. Из-за недостаточного внимания к мерам контроля часто проваливаются хорошие планы. Обилие планов при недостаточном контроле за их выполнением является признаком бюрократии, для которой разработка разнообразных планов становится самоцелью.

В общем случае для эффективного управления силами и средствами системы инженерно-технической защиты информации необходимо обеспечить:

• прогноз угроз;

• данные о состоянии сил и средств системы;

• модели объектов защиты и угроз;

• данные о выявленных технических каналов утечки информации;

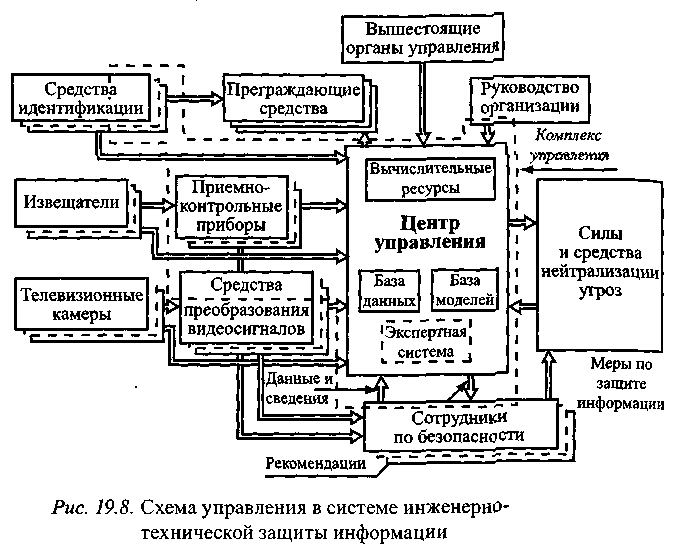
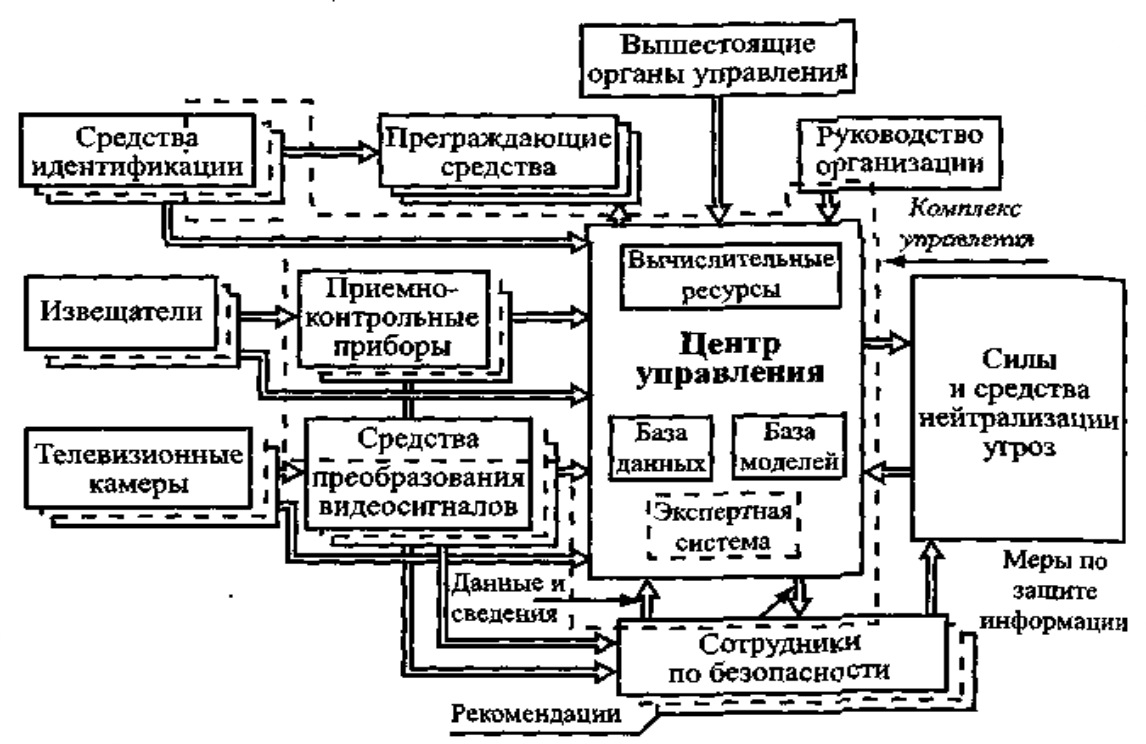
• решения о мерах нейтрализации угроз в случае появления сигналов тревоги и других сигналов, требующих реагирования (например, об обрыве шлейфа);

• реализацию решений в виде команд силам и средствам нейтрализации угроз;

• контроль за посетителями организации;

• контроль за эффективностью принятых мер защиты.

Так как управление силами и средствами инженерно-технической защиты включает разнообразные специфические процессы, для выполнения которых необходимы соответствующие программно-аппаратные средства и специалисты, то объективно система инженерно-технической защиты информации должна иметь комплекс управления.



1. **Разработка технической системы защиты информации объекта.**

Способы и средства **технической защиты информации** применяются для создания системы защиты информации, препятствующей реализации угроз утечки информации по техническим каналам. 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 – 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.

***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.

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 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;
* 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 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 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.



1. **Моделирование объектов защиты**

Одним из главных этапов разработки технической системы защиты информации является моделирование объектов защиты.

Моделирование объектов защиты включает:

* структурирование защищаемой информации;
* разработку моделей объектов защиты.

Для структурирования информации в качестве исходных данных используются:

* перечень сведений, составляющих государственную, ведомственную или коммерческую тайну;
* перечень источников информации в организации.

**Структурирование информации** проводится путем классификации информации в соответствии со структурой, функциями и задачами организации с привязкой элементов информации к ее источникам.

Задача моделирования объектов защиты состоит в объективном описании и анализе источников конфиденциальной информации и существующей системы ее защиты. Для построения точной модели объекта защиты необходимо:

* определение источников защищаемой информации;
* описание пространственного расположения основных мест размещения источников защищаемой информации;
* выявление путей распространения носителей с защищаемой информации за пределы контролируемых зон (помещений, зданий, территории организации);
* описание с указанием характеристик существующих преград на путях распространения носителей с информацией за пределы контролируемых зон.

Моделирование проводится на основе пространственных моделей контролируемых зон с указанием мест расположения источников защищаемой информации – планов помещений, этажей зданий, территории в целом. На планах помещений указываются в масштабе места размещения ограждений, экранов, воздухопроводов, батарей и труб отопления, элементов интерьера и других конструктивных элементов, способствующих или затрудняющих распространение сигналов с защищаемой информацией, а также места размещения и зоны действия технических средств охраны и телевизионного наблюдения. Их параметры целесообразно объединить в таблице, вариант которой приведен в таблице 2.

На планах этажей здания указываются выделенные (с защищаемой информацией) и соседние помещения, схемы трубопроводов водяного отопления, воздухопроводов вентиляции, кабелей электропроводки, телефонной и вычислительной сетей, радиотрансляции, заземления, зоны освещенности дежурного освещения, места размещения и зоны наблюдения телевизионных камер и т. д.

На плане территории организации отмечаются места размещения здания (зданий), забора, контрольно-пропускного пункта, граничащие с территорией улицы и здания, места размещения и зоны действия технических средств охраны, телевизионной системы наблюдения и наружного освещения, места вывода из организации кабелей, по которым могут передаваться сигналы с информацией.

В процессе моделирования необходимо выполнить анализ возможных путей распространения информации за пределы контролируемой зоны и определить уровни сигналов на их границах на основе рассмотренных пространственных моделей. В результате моделирования определяется состояние безопасности информации и слабые места существующей системы ее защиты. Результаты моделирования оформляются на планах и в таблицах.

# 34. Моделирование угроз и каналов утечки информации

*Моделирование угроз безопасности информации* предусматривает анализ способов ее хищения, изменения и уничтожения с целью оценки наносимого этими способами ущерба.

*Моделирование угроз включает*:

* моделирование способов физического проникновения злоумышленника к источникам информации;
* моделирование технических каналов утечки информации.

Действия злоумышленника по добыванию информации, как и других материальных ценностей, определяются поставленными целями и задачами, его мотивами, квалификацией и технической оснащенностью.

*Для создания модели угрозы физического проникновения*, достаточно близкой к реальной, необходимо попытаться мысленно проиграть с позиции злоумышленника варианты проникновения к источнику информации.

*Модель злоумышленника*выглядит следующим образом:

1. злоумышленник представляет собой серьезного противника, тщательно готовящего операцию проникновения;
2. имеет в распоряжении современные технические средства проникновения и преодоления механических преград;
3. всеми доступными способами добывает и анализирует информацию о расположении зданий и помещений организации, о рубежах охраны, о местах хранения источников информации, видах и типах средств охраны, телевизионного наблюдения, освещения и местах их установки;
4. проводит анализ возможных путей проникновения к источникам информации и ухода после выполнения задачи.

*Злоумышленников разделяют на следующие типы*:

1. *неподготовленный*, который ограничивается внешним осмотром объекта. проникает в организацию через двери и окна, при срабатывании тревожной сигнализации убегает;
2. *подготовленный*, изучающий систему охраны объекта и готовящий несколько вариантов проникновения в организацию, в основном, путем взлома инженерных конструкций;
3. *квалифицированный*, который тщательно готовится к проникновению, выводит из строя технические средства охраны, применяет наиболее эффективные способы проникновения.

Возможные пути проникновения злоумышленников отмечаются линиями на планах (схемах) территории, этажей и помещений зданий, а результаты анализа пути заносятся в таблицу:



В качестве достаточно общих индикаторов каналов утечки информации могут служить указанные в таблице 4 демаскирующие признаки.

|  |  |
| --- | --- |
| Вид канала | Индикаторы |
| Оптический | Окна, выходящие на улицу, близость к ним домов и деревьев. Отсутствие на окнах занавесок, штор, жалюзи. Читаемость содержания документов на столах. Читаемость содержания плакатов на стенах помещения. Малое расстояние между столами сотрудников в помещении. Читаемость экранов мониторов ПЭВМ на столах сотрудников со стороны окон, дверей или других сотрудников. Появление возле территории организации посторонних людей (в том числе в автомобилях) с биноклями, фотоаппаратами, кино и видеокамерами. |
| Радио-электронный | Наличие в помещении радиоэлектронных средств, ПЭВМ. ТА городской и внутренней АТС, громкоговорителей трансляционной сети и других предметов. Применение средств радиосвязи. Параллельное размещение кабелей в одном жгуте при разводке их внутри здания и на территории организации. Отсутствие заземления радио и электрических приборов. |
| Акустический | Малая толщина дверей и стен помещения. Наличие в помещении открытых вентиляционный отверстий. Отсутствие экранов на отопительных батареях. Близость окон к улице и ее домам. Появление возле организации людей с достаточно большими сумками, длинными и толстыми зонтами. Частая и продолжительная парковка возле организации чужих автомобилей. |
| Материально-вещественный | Наличие закрытых и опечатанных ящиков для бумаги и твердых отходов с демаскирующими веществами. Применение радиоактивных веществ. Неконтролируемый выброс газов с демаскирующими веществами, слив в водоемы и вывоз на свалку твердых отходов. Запись сотрудниками конфиденциальной информации на неучтенных листах бумаги. |

Потенциальные каналы утечки определяются для каждого источника информации, причем их количество может не ограничиваться одним или двумя.

От источника информации – руководителя фирмы – утечка информации возможна по следующим каналам:

- через дверь в приемную или коридор;

- через окно на улицу или во двор;

- через вентиляционное отверстие в соседние помещения;

- с опасными сигналами по радиоканалу;

- с опасными сигналами по кабелям, выходящим из помещения;

- по трубам отопления в другие помещения здания;

- через стены, потолок и пол в соседние помещения;

- с помощью закладных устройств за территорию фирмы.

Применительно к моделям каналов утечки информации целесообразно иметь модели, описывающие каналы в статике и динамике.

*Статическое состояние канала* характеризуют *структурная и пространственная модели*.

**Структурная модель** описывает структуру (состав и связи элементов) канала утечки.

**Пространственная модель** содержит описание положения канала утечки в пространстве.

Динамику **канала утечки информации** описывают *функциональная и информационная модели*.

**Функциональная модель** характеризует режимы функционирования канала, интервалы времени, в течение которых возможна утечка информации, а **информационная** содержит характеристики информации, утечка которой возможна по рассматриваемому каналу: количество и ценность информации, пропускная способность канала, прогнозируемое качество принимаемой злоумышленником информации.

Каждый вид канала содержит свой набор показателей источника и приемника сигналов в канале.

При описании **приемника сигнала** необходимо учитывать реальные возможности злоумышленника.

**Оценки угроз информации** в результате проникновения злоумышленника к источнику или ее утечки по техническому каналу проводятся с учетом меры (вероятности) **Рр** реализуемости рассматриваемого пути или канала, а также цены соответствующего элемента информации **Си.**

Угроза безопасности информации, выраженной в величине ущерба **Суи** от попадания ее к злоумышленнику, определяется для каждого пути или канала в виде **Суи = Си \* Рр.**

# 35. Рекомендации по выбору методов и средств технической защиты информации

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.



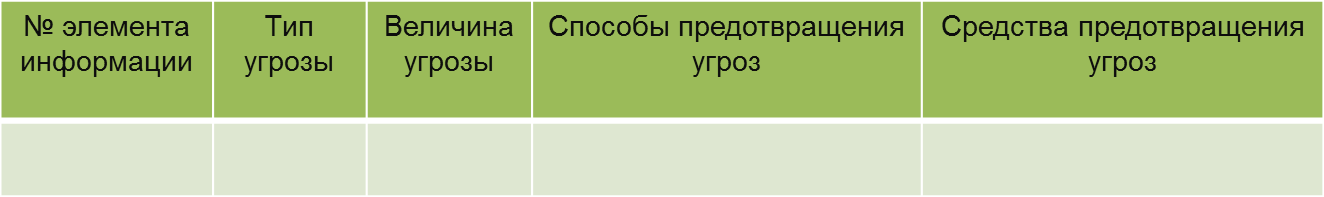
Разработка мер по предотвращению угроз представляет собой итерационный процесс, каждая итерация которого выполняется в 2 этапа:

* 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.

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

Рекомендуемые способы и средства защиты информации заносятся в таблицу, вариант которой приведен в таблице:



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

# 36. САПР систем технической защиты информации

Для наиболее качественного и менее трудоемкого проектирования инженерно-технической системы защиты информации (ИТСЗИ) в современных условиях необходимо применять специализированную объектно-ориентированную **систему автоматизированного проектирования** – САПР ИТСЗИ.

Создание подобной системы, способной моделировать, проектировать и оптимизировать инженерно-техническую защиту объекта, позволяет:

* адекватно и своевременно противодействовать злоумышленникам.
* повышать качество принимаемых решений при создании системы защиты.
* осуществлять оптимальный выбор средств защиты информации.
* сократить время на проектирование и ввод в эксплуатацию системы защиты.
* качественно подготовить документацию, необходимую для проектирования, монтажа и эксплуатации средств защиты.

Модель защищаемого объекта (кабинет, этаж, здание, прилегающая территория) должна быть представлена в САПР ИТСЗИ в виде некоторой структуры данных.

Свойствами этой структуры являются наиболее важные характеристики объекта такие, как:

* Этажность
* площадь защищаемого объекта
* толщина перекрытий
* типы остекления
* количество входов
* и т.д.

В состав системы входят следующие программно-методические модули:

* ввода данных, предназначенный для ввода исходных данных об объекте защиты и описания характеристик элементов объекта, получаемых в результате проведения аудита информационной безопасности объекта защиты;
* моделирования объекта защиты и источников информации, предназначенный для моделирования объекта защиты и определения источников информации;
* внутреннего представления модели защищаемого объекта, предназначенный для преобразования исходных данных и модели объекта защиты в универсальный формат, доступный всем проектным модулям САПР ИТСЗИ;
* проектный, отвечающий за определённый вид защиты (противопожарная система, система контроля и управления доступом, система охраны, физическая защита вычислительных мощностей и т.д.);
* моделирования угроз и определения каналов утечки информации, предназначенный для определения всех вероятных угроз информации;
* выбора средств ИТЗИ, осуществляющий по критерию выбор методов и средств защиты информации из базы данных;
* база данных технических средств, содержащий перечень методов и средств защиты информации и их характеристики, включающий следующие разделы: технические средства охраны, пожарная сигнализация, телевизионные системы видеонаблюдения, системы контроля и управления доступом, инженерные конструкции и сооружения;
* оптимального выбора средств ИТЗИ, предназначенный для анализа и оптимального выбора комбинации технических средств защиты информации;
* разработки организационно-технического обеспечения, предназначенный для разработки организационно-правовой и технической сопроводительной документации проекта ИТСЗИ;
* формирования ИТСЗИ, формирующий законченный проект инженерно-технической укрепленности и предоставляющий статистические данные по защите объекта.
* документирования и сохранения проекта, служащий для документирования, сохранения и дальнейшего использования результатов проектирования.

# 37. 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
* организацию режима охраны на удалении, обеспечивающего скрытность деятельности.

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

# 38. Способы и средства противодействия наблюдению в оптическом диапазоне волн.

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**.

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.

*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.

*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.

При *имитационном окрашивании* цвет и характер пятен на поверхности объекта подбирается под расцветку окружающей местности, объектов или предметов в месте расположения защищаемого объекта.

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

**Маски-навесы** предназначены для скрытия объектов, расположенных на открытых сверху площадках и защищают их от наблюдения сверху.

**Вертикальные маски** защищают объекты от наблюдения с земли.

**Наклонные маски** используются в основном для скрытия теней объемных объектов.

**Радиопрозрачные маски** выполняются из радиопрозрачных материалов 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 из подручных материалов (хвороста, камыша, тростника, кустарника) или из табельных средств и материалов (маскировочной сети, армированной маскировочной бумаги, сетчатой ткани, полихлорвиниловой пленки и др.), а также в виде различных сборных возимых маскировочных комплектов.

**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).

**Энергетическое скрытие демаскирующих признаков объектов** достигается путем уменьшения яркости объекта и фона ниже чувствительности глаза или технического фотоприемника, а также их ослепление.

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.

# 39. Способы информационного скрытия объектов от радиолокационного наблюдения.

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 генерирования радиопомех.

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

***Энергетическое скрытие достигается*** за счет уменьшения эффективной площади рассеяния объекта в основном двумя способами: изменением диаграммы направленности отражающей поверхности объекта и поглощением облучающей энергии радиолокатора.

***Градиентное поглощение обеспечивают многослойные материалы***, каждый слой которых состоит из основы - диэлектрика и наполнителя, поглощающих электромагнитную энергию.

Другой вид радиопоглощающего материала использует ***эффект интерференции прямой (падающей) и отраженной от объекта электромагнитных волн***.

Другой способ энергетического скрытия, который широко применяется для защиты объектов от радиолокационного наблюдения, - **генерация помех**.

Защита информации об объектах, находящихся в воде, предусматривает, прежде всего, защиту от гидроакустического наблюдения. 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;
* создание активных помех гидролокаторам, в том числе путем ретрансляции облучающих сигналов с усилением их мощности.

# 40. Способы защиты информации при передаче ее по оптоволоконному кабелю.

Есть три основных категории методов предотвращающих или снижающих до минимума влияние посторонних подключений:

**A. Наблюдение за кабелем и мониторинг.**

1. Мониторинг сигналов вблизи волокна.

Производство оптоволокна с дополнительными волокнами, по которым передается специальный сигнал мониторинга. Использование такого метода увеличит стоимость кабеля, но любая попытка согнуть кабель вызывает потерю сигнала мониторинга, и вызывает срабатывание сигнала тревоги [7].

2) Электрические проводники

Другой метод состоит в интегрировании электрических проводников в кабель, и если оболочка кабеля нарушена, то изменяется емкость между электрическими проводниками и это может использоваться для срабатывания тревоги.

3) Мониторинг мощности мод.

Этот метод применим к мультимодовому волокну, в котором затухание – это функция от моды, в которой распространяется свет. Подсоединение влияет на определенные моды, но при этом затрагивает и другие моды. Это приводит к перераспределению энергии от проводящих мод к непроводящим, что меняет соотношение энергии в ядре волокна и его оболочке. Изменение энергии в модах может быть обнаружено на принимающей стороне соответствующим измерением, что будет являться информацией для принятия решения – есть подключение к кабелю или нет [8].

4) Измерение оптически значимой мощности

В волокне может осуществляться мониторинг уровня оптически значимой мощности. В том случае, если она отличается от установленного значения, срабатывает сигнал тревоги. Однако это требует соответствующей кодировки сигнала, так чтобы в волокне присутствовал постоянный уровень сигнала, не зависящий от наличия передаваемой информации [8].

5) Оптические рефлектометры

Поскольку подсоединение к волокну забирает часть оптического сигнала, для обнаружения подключений могут использоваться оптические рефлектометры. С их помощью можно установить расстояние по трассе, на котором обнаруживается падение уровня сигнала[8].

6) Методы с использованием пилотного тона:

Пилотные тоны проходят по волокну также как и коммуникационные данные. Они используются для обнаружения перерывов в передаче. Пилотные тоны могут использоваться для обнаружения атак, связанных с постановкой помех, но если несущие волновые частоты пилотных тонов не затрагиваются, то данный метод не является эффективным при обнаружении такого рода атак. О наличии подключения можно судить только по существенной деградации уровня сигнала пилотного тона [8]

**B. Сильногнущееся волокно.**

Эти виды волокна, обычно называемые волокном с низкими потерями и сильным радиусом изгиба, защищают сеть передачи данных, ограничивая высокие потери, возникающие при прокалывании волокна или его сгибании. Кроме того, для светового потока становятся менее повреждающими такие факторы как вытягивание, перекручивание и другие физические манипуляции с волокном. Существуют также другие типы волокна основанные на иных технологиях производства [9].

**C. Шифрование**

Хотя шифрование никак не препятствует подсоединению к волокну, она делает украденную информацию малополезной для злоумышленников.

# 41. Классификация объектов информатизации.

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** (*специальные требования и рекомендации по технической защите конфиденциальной информации*) являются:

* **средства и системы информатизации, используемые для обработки конфиденциальной информации:**
  + 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);
* **технические средства и системы, не обрабатывающие непосредственно конфиденциальную информацию, но размещенные в помещениях, где она обрабатывается** (циркулирует);
* **защищаемые помещения.**

# 42. Экранирование технических средств и их соединительных линий.

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

Наряду c 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*.

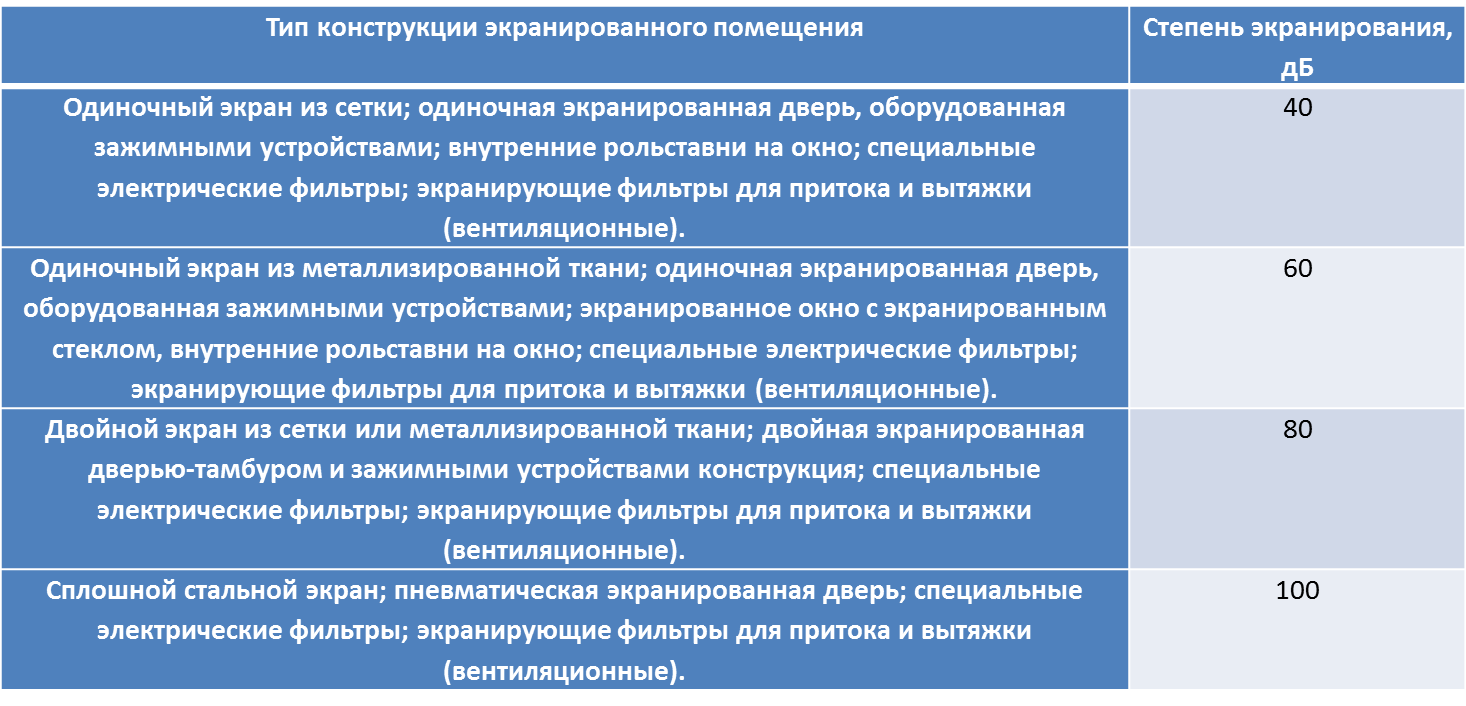
*Для экранирования магнитного поля проводов необходимо создать поле такой же величины и обратного направления.* С этой целью необходимо весь обратный ток экранируемой цепи направить через экранирующую оплётку провода. Для полного осуществления этого принципа необходимо, чтобы экранирующая оболочка была единственным путём для протекания обратного тока.

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.

*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)*.

# 43. Экранированные помещения.

* В обычных (неэкранированных) помещениях основной экранирующий эффект обеспечивают железобетонные стены домов.
* Как правило, степень экранирования обычных помещений невысока вследствие наличия в них окон, дверей и вентиляционных отверстий, поэтому их экранированию необходимо уделять первостепенное внимание.



Для экранирования дверей в основном используется листовая сталь, а на окна устанавливается одно или двухслойная медная сетка с ячейкой не более 2x2 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.

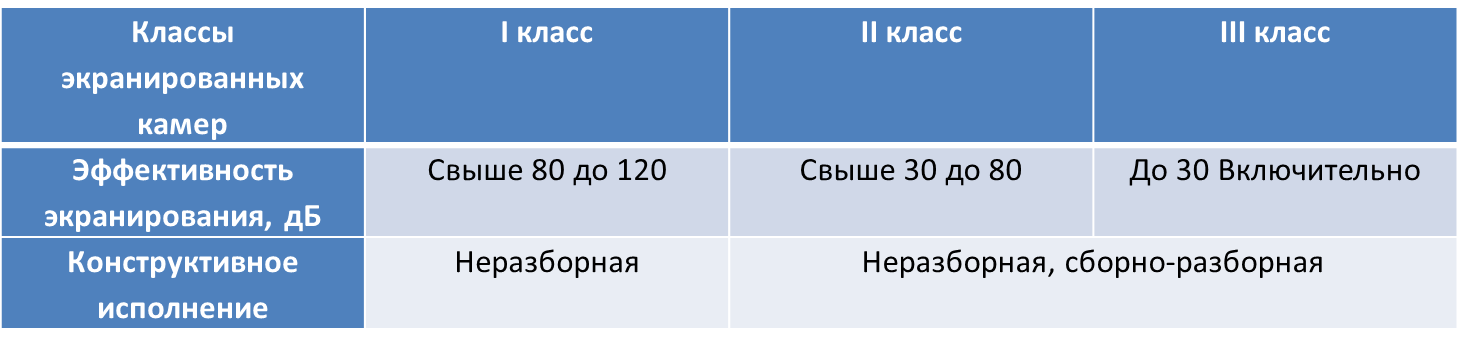
На практике экранировку электромагнитных волн более 60 дБ можно обеспечить только в *специальных экранированных сооружениях* (ЭС) или в *экранированных камерах* (ЭК).

Выполняются экранированные сооружения из стальных сплошных листов, соединённых электродуговой сваркой.

При закрытии экранированной двери должен обеспечиваться надёжный электрический контакт со стенками помещения (с дверной рамой) по всему периметру.

*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.

В зависимости от эффективности экранирования и конструктивного исполнения ЭК подразделяют на три класса.



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.

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.

РЧФ устанавливают в местах ввода в ЭК сетей освещения, силовых низковольтных и высоковольтных сетей, цепей управления, блокировки, сигнализации, связи и т. д.

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.

Для изготовления ЭК должны применяться только несгораемые и трудносгораемые отделочные материалы.

Двери ЭК должны открываться по ходу эвакуации.

В ЭК площадью более 100 м2 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.

# 44. Заземление технических средств.

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.

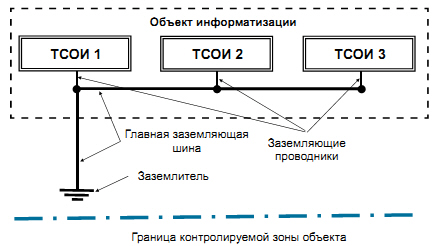
Заземлитель - проводящая часть (заземляющий электрод) или совокупность соединённых между собой проводящих частей, находящихся в электрическом контакте с землёй непосредственно или через промежуточную проводящую среду.

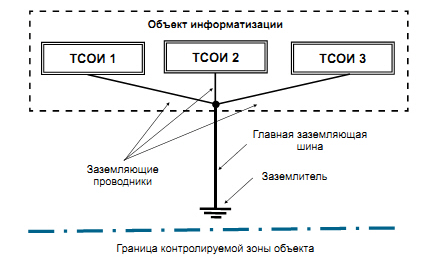
Заземление делится на два основных вида по выполняемой роли - рабочее (функциональное) и защитное.

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).

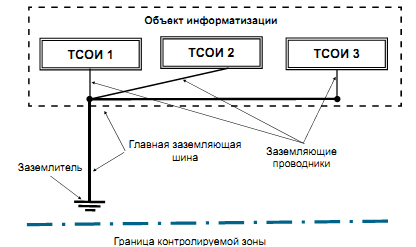
**Заземление, используемое в целях электромагнитного экранирования, относится к рабочему заземлению**, но оно выполняет также функции и защитного заземления.

В большинстве случаев все ТСОИ, установленные на объекте информатизации, заземляются на один общий заземлитель (одноточечная схема заземления).



**Одноточечная последовательная схема заземления** наиболее проста. 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** 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.

Заземление экранов ТСОИ должно быть выполнено в соответствии с определёнными правилами. Основные требования, предъявляемые к системе рабочего заземления объекта информатизации, заключаются в следующем:

* система заземления должна включать заземлитель, шину заземления и заземляющие проводники, соединяющие за-землитель с экранами ТСОИ и их информативных кабелей;
* запрещается использовать в качестве заземляющего устройства провода электросетей (нулевые фазы), металлоконструкции зданий, металлические оболочки подземных кабелей, металлические трубы систем отопления, водоснабжения, канализации;
* главная заземляющая шина должна проходить как можно ближе к ТСОИ и быть соединена с его экраном заземляющим проводником наименьшей длины;
* 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;
* общее сопротивление заземлителя, заземляющих проводников и шин заземления не должно превышать 4 Ом;
* каждый заземляемый элемент должен быть присоединён к заземлителю или к шине заземления при помощи отдельного проводника .

Последовательное включение в заземляющий проводник заземляемых технических средств не допускается.

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).

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.

**45) Требования к системам электропитания и заземления основных технических средств и систем**

В целях защиты информации от её утечки по цепям электропитания к системе электропитания объектов информатизации (ОИ) предъявляются определённые требования, к основным из которых относятся следующие:

* электропитание ОИ рекомендуется осуществлять от трансформаторной подстанции, расположенной в пределах контролируемой зоны объекта;
* подключение к распределительному устройству трансформаторной подстанции, питающей объект информатизации, посторонних потребителей, расположенных за пределами контролируемой зоны, должно быть исключено;
* линии электропередачи от подстанции до вводно-распределительного или вводного устройства, установленного в здании, должны прокладываться экранированными (бронированными) кабелями и не должны иметь выходов за пределы контролируемой зоны;
* помещения, в которых установлены распределительные устройства и силовые щиты, а также сами силовые щиты должны закрываться на замки и опечатываться;
* подключение электропитания СВТ, установленных на объекте информатизации, предпочтительно осуществлять от одной фазы или от отдельного щитка. Причём к этой фазе (или щитку) не следует подключать вспомогательные технические средства и системы (ВТСС);
* при совместной прокладке кабелей электропитания СВТ с проводами и кабелями, имеющими выход за пределы контролируемой зоны объекта, расстояние между ними должно быть не менее 0,1 м. При невозможности выполнения этого требования линии электропитания СВТ должны прокладываться экранированными кабелями или в экранированных коробах;
* заземляющие устройства как трансформаторной подстанции, так и объекта информатизации должны находиться в пределах контролируемой зоны объекта не ближе 10 м от её границы;
* все заземляющие проводники должны прокладываться изолированными проводами и кабелями;
* общее сопротивление заземлителя, заземляющих проводников и шин заземления не должно превышать 4 Ом.

Заземление технических средств систем управления, связи и автоматизации должно быть выполнено в соответствии с определенными правилами. Основные требования, предъявляемые к системе заземления, заключаются в следующем:

* - система заземления должна включать общий заземлитель, заземляющий кабель, шины и провода, соединяющие заземлитель с объектом;
* - сопротивления заземляющих проводников, а также земляных шин должны быть незначительными;
* - каждый заземляемый элемент должен быть присоединен к заземлителю или к заземляющей магистрали при помощи отдельного ответвления; последовательное включение в заземляющий проводник нескольких заземляемых элементов запрещается;
* - в системе заземления должны по возможности отсутствовать замкнутые контуры, образованные соединениями или нежелательными связями между сигнальными цепями и корпусами устройств, между корпусами устройств и землей;
* - следует избегать использования общих проводников в системах экранирующих заземлений, защитных заземлений и сигнальных цепей;
* - качество электрических соединений в системе заземления должно обеспечивать минимальное сопротивление контакта, надежность и механическую прочность контакта в условиях климатических воздействий и механических нагрузок;
* - контактные соединения должны исключать возможность образования оксидных пленок на контактирующих поверхностях и связанных с этими пленками нелинейных явлений;
* - контактные соединения должны исключать возможность образования гальванических пар для предотвращения коррозии в цепях заземления;
* - запрещается использовать в качестве заземляющего устройства нулевые фазы электросетей, металлоконструкции зданий, трубы систем отопления, водоснабжения, канализации и т. д.

**46) Помехоподавляющие фильтры (принципы построения, основные характеристики, требования по установке).**

Фильтры помехоподавляющие электрические 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.

Фильтры помехоподавляющие электрические:

а) типа ФП (индуктивно-ёмкостные многопроводные);

б) типа ФСПП (на основе электродинамических замедляющих структур, однопроводные и многопроводные)

**47) Классификация помех по природе возникновения и характеристикам.**

Помехи

Естественные

Искусственные

Земные

Внеземные

Непреднамеренные

Преднамеренные

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.

**48) Системы пространственного электромагнитного зашумления (принципы построения, основные характеристики, требования по установке)**

К **системе пространственного зашумления**, применяемой для создания маскирующих электромагнитных помех, предъявляются следующие требования:      • система должна создавать электромагнитные помехи в диапазоне частот возможных побочных электромагнитных излучений ТСПИ;      • создаваемые помехи не должны иметь регулярной структуры;      • уровень создаваемых помех (как по электрической, так и по магнитной составляющей поля) должен обеспечить отношение с/ш на границе контролируемой зоны меньше допустимого значения во всем диапазоне частот возможных побочных электромагнитных излучений ТСПИ;      • система должна создавать помехи как с горизонтальной, так и с вертикальной поляризацией (поэтому выбору антенн для генераторов помех уделяется особое внимание);      • на границе контролируемой зоны уровень помех, создаваемых системой пространственного зашумления, не должен превышать требуемых норм по ЭМС.      Цель пространственного зашумления считается достигнутой, если отношение опасный сигнал/шум на границе контролируемой зоны не превышает некоторого допустимого значения, рассчитываемого по специальным методикам для каждой частоты информационного (опасного) побочного электромагнитного излучения ТСПИ .      В системах пространственного зашумления в основном используются помехи типа "белого шума" или "синфазные помехи" .      Системы, реализующие метод "синфазной помехи", в основном применяются для защиты ПЭВМ. В них в качестве помехового сигнала используются импульсы случайной амплитуды, совпадающие (синхронизированные) по форме и времени существования с импульсами полезного сигнала. Вследствие этого по своему спектральному составу помеховый сигнал аналогичен спектру побочных электромагнитных излучений ПЭВМ. То есть, система зашумления генерирует "имитационную помеху", по спектральному составу соответствующую скрываемому сигналу .      В настоящее время в основном применяются системы пространственного зашумления, использующие помехи типа "белый шум", то есть излучающие широкополосный шумовой сигнал (как правило, с равномерно распределенным энергетическим спектром во всем рабочем диапазоне частот), существенно превышающий уровни побочных электромагнитных излучений

**49)  Системы линейного электромагнитного зашумления (принципы построения, основные характеристики, требования по установке).**

**Системы линейного зашумления** применяются для маскировки наведенных опасных сигналов в посторонних проводниках и соединительных линиях ВТСС, выходящих за пределы контролируемой зоны. Они используются в том случае, если не обеспечивается требуемый разнос этих проводников и ТСПИ (то есть не выполняется требование по Зоне № 1), однако при этом обеспечивается требование по Зоне № 2 (то есть расстояние от ТСПИ до границы контролируемой зоны больше, чем Зона № 2).      В простейшем случае система линейного зашумления представляет собой генератор шумового сигнала, формирующий шумовое маскирующее напряжение с заданными спектральными, временными и энергетическими характеристиками, который гальванически подключается в зашумляемую линию (посторонний проводник). Характеристики некоторых генераторов шума, используемых в системах линейного зашумления, представлены в табл. 2.8.       На практике наиболее часто подобные системы используются для зашумления линий электропитания (например, линий электропитания осветительной и розеточной сетей).

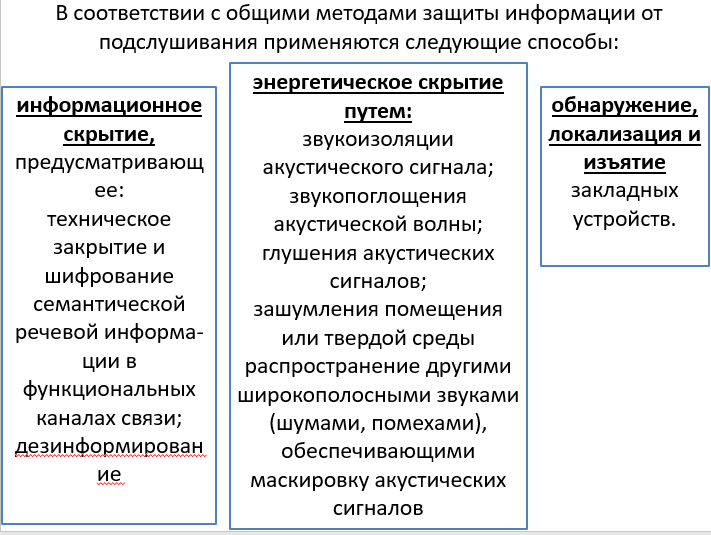
К системе линейного зашумле­ния, применяемой для создания ма­скирующих электромагнитных по­мех в цепях электропитания СВТ, предъявляются следующие требова­ния:

• система должна создавать элек­тромагнитные помехи в диапазоне частот возможных наводок побоч­

ных электромагнитных излучении СВТ (от 150 кГц до 300 МГц);

* создаваемые помехи не должны иметь регулярной структуры (энт­ропийный коэффициент качества шума должен быть не менее 0,6);
* уровень создаваемых помех дол­жен обеспечить отношение сиг­нал/шум в зашумляемой линии электропитания СВТ на границе контролируемой зоны не более допустимого значения (δ) во всем диапазоне частот возможных на­водок побочных электромагнит­ных излучений СВТ;
* система должна иметь сертифи­кат по требованиям безопаснос­ти информации ФСТЭК РФ.

В системах линейного зашумле­ния в основном используются по­мехи типа «белого шума» с равно­мерно распределенным энергетиче­ским спектром во всем рабочем диа­пазоне частот.

**50) Способы и принципы работы средств защиты информации от подслушивания.**

**Информационное скрытие** речевой информации обеспечивается техниче­ским закрытием (аналоговым скремблированием) и шифрованием сигналов речевой информации, передаваемых по кабелям и радиоканалам.

**Энергетическое скрытие** достигается уменьшением отношения энергии (мощности) сигналов, т. е. носителей (электромагнитного или акустического полей и электрического тока) с информацией, и помех. Уменьшение отноше­ния сигнал/помеха (слово «мощность», как правило, опускается) возможно двумя методами: снижением мощности сигнала или увеличением мощности помехи на входе приемника.

**обнаружение, локализация и изъятие**  Воздействие помех приводит к изменению информационных параметров носителей: амплитуды, частоты, фазы. Если носителем информации является амплитудно-модулированная электромагнитная волна, а в среде распростра­нения канала присутствует помеха в виде электромагнитной волны, имеющая одинаковую с носителем частоту, но случайную амплитуду и фазу, то проис­ходит интерференция этих волн. В результате этого значения информацион­ного параметра (амплитуды суммарного сигнала) случайным образом изме­няются и информация искажается. Чем меньше отношение мощностей, а сле­довательно, амплитуд, сигнала и помехи, тем значительнее значения ампли­туды суммарного сигнала будут отличаться от исходных (устанавливаемых при модуляции) и тем больше будет искажаться информация.

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.

**51) Классификация, сущность и параметры звукоизоляции ограждений, кабин, акустических экранов**

**Звукоизолирующие ограждения**помещений и зданий — это стены, перекрытия, перегородки, окна, двери, имеющие по пери­метру контакты с другими ограждениями. Величина звукоизоля­ции однослойного ограждения характеризуется сложной нелиней­ной зависимостью как от частоты f колебания акустической вол­ны, так и от большой группы характеристик ограждения. В общем случае эту зависимость можно представить в виде следующей фун­кции:

R = F(f3B,m,h/for,p,v),

где m — поверхностная масса (масса 1 м2) ограждения; h — коэф­фициент потерь энергии в материале; for —собственная частота ко­лебаний ограждения; р — удельная плотность материала огражде­ния; v — скорость звука в материале ограждения.

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, соединенными ребрами жесткости, помещают различные звукопоглощающие материалы.

Значения ослабления звука ограждениями (стенами и меж­этажными перекрытиями), выполненными из некоторых часто при­меняемых строительных конструкций

Одними 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. Повышение звукоизоляции дверей обеспечивается:

•устранением щелей между дверью и дверной коробкой путем применения уплотняющих прокладок из резины, порога или ре­зинового фартука между дверью и полом;

•применением для дверного полотна более плотных пород дере­ва, увеличением толщины дверного полотна и обивки его де­рматином или аналогичным материалом по слою войлока или ваты с валиком по периметру двери;

•установкой звукоизолирующей двери, выполненной в виде мно­гослойного дверного полотна с размещением между слоями зву­коизолирующего материала;

•установкой двойных дверей с тамбуром между ними шириной 20-30 см.

**52) Понятность и разборчивость речи.**

*Понятность речи*— основная характеристика, определяющая пригодность тракта для передачи речи. Непосредственное определение этой характеристики может быть осуществлено статистическим методом с привлечением большого числа слушателей и дикторов. Количественное определение понятности речи –*разборчивость*.

*Разборчивостью речи*называют относительное или процентное число правильно принятых элементов речи из общего числа переданных по тракту. Элементы речи – сложные звуки, слова, фразы, цифры. Соответственно различают *слоговую, звуковую, словесную, смысловую и цифровую разборчивости.*Между ними существует статистическая взаимосвязь. В практике преимущественно используют слоговую, словесную и смысловую разборчивости.

Для измерений разборчивости разработаны специальные таблицы слогов с учетом встречаемости их в русской речи. Эти таблицы называются*артикуляционными.*Разборчивость измеряют с помощью тренированной бригады слушателей без нарушений слуха и речи путем проведения субъективно-статистических экспертиз. При этом измерения могут проводиться различными методами, например, методом бальной оценки, методом определения процента правильно принятых слов и т.д.

Причинами снижения разборчивости являются акустические шумы в помещении, помехи от реверберации и диффузного звука, недостаточное усиление сигналов первичного источника звука.

Системы озвучения и звукоусиления должны обеспечивать требуемую понятность речи. При передаче информационных программ, проведении митингов и собраний необходима отличная понятность речи, которая обеспечивается при 80 % слоговой и 98 % словесной разборчивостях. Для диспетчерской связи полная разборчивость речи (удовлетворительная понятность) получается при 40...50 % слоговой и 87...93 % словесной разборчивостях. Поэтому при расчете диспетчерской связи ориентируются на меньшие величины разборчивости, чем при расчетах систем широкого применения.

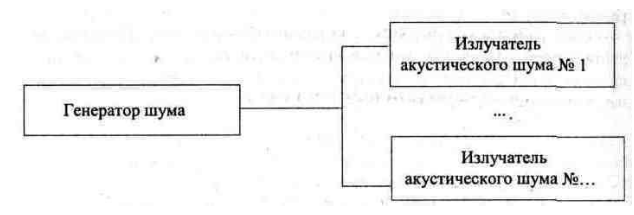
Существует связь между разборчивостью речи, условиями приема и характеристиками трактов передачи, которую удалось установить при помощи формантной теории, разработанной Флетчером и Коллардом.

Области концентрации энергии в том или ином участке частотного диапазона называются *формантами.*Их расположение зависит как от положения звука в слове или фразе, так и от индивидуальных особенностей артикуляционного аппарата человека. Каждый звук имеет несколько формант. Форманты звуков речи заполняют частотный диапазон от 150 до 7000 Гц.

**53) Генераторы акустического и виброакустического шума.**

Генераторы шума в речевом диапазоне получили достаточно широкое распространение в практике защиты информации. Они используются для защиты от несанкционированного съема акустической информации путем маскирования непосредственно полезного звукового сигнала. Маскирование проводится «белым» шумом с корректированной спектральной характеристикой.

Примерный вид структурной схемы источника акустического шума приведен на рис. 2.4.14. Конструктивно аппаратура включает блок формирования и усиления шумового сигнала и несколько акустических излучателей.

Главный недостаток применения источников шумов в акустическом диапазоне - это невозможность комфортного проведения переговоров. Практика показывает, что в помещении где «ревет» генератор шума невозможно находиться более 10... 15 мин. Кроме того, собеседники автоматически начинают пытаться перекричать средство защиты, снижая эффективность его применения. Поэтому подобные системы применяются для дополнительной защиты дверных проемов, межрамного пространства окон, систем вентиляции и т. д.

Наиболее эффективным средством защиты помещений, предназначенных для проведения конфиденциальных мероприятий, от съема информации через оконные стекла, стены, системы вентиляции, трубы отопления, двери и т. д. являются устройства виброакустической защиты. Данная аппаратура позволяет в некоторых случаях предотвратить возможное прослушивания с помощью

проводных микрофонов, звукозаписывающей аппаратуры, радиомикрофонов и электронных стетоскопов, лазерного съема акустической информации с окон и т. д. Противодействие прослушиванию обеспечивается внесением виброакус-тйческих шумовых колебаний в элементы конструкции здания.

Генератор формирует «белый» шум в диапазоне звуковых частот. Передача акустических колебаний на ограждающие конструкции производится при помощи пьезоэлектрических (на основе пьезокерамики) или электромагнитных вибраторов с элементами крепления. Конструкция и частотный диапазон излучателей должны обеспечивать эффективную передачу вибрации. Вибропреобразователи возбуждают шумовые виброколебания в ограждающих конструкциях, обеспечивая при этом минимальный уровень помехового акустического сигнала в помещении, практически не влияющий на комфортность проведения переговоров.

Предусмотренная в большинстве изделий возможность подключения акустических излучателей, позволяет «зашумлять» вентиляционные каналы и дверные тамбуры. Как правило, имеется возможность плавной регулировки уровня шумового акустического сигнала.

**54) Способы и средства предотвращения утечки информации с помощью закладных устройств.**

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:**

**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.

**55) Методика оценки возможностей средств акустической разведки по перехвату речевой информации.**

**Уровень звукового давления** отношение величины звукового давления Р к нулевому уровню, за который принято звуковое давление Р= 2 ⋅ 10-5 Н/м2

N = 20 lg P/Р0

***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 I0= 10–12 Вт/м2, выраженное в децибелах (дБ)*

N = 10 lg I/ I0

**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 ⋅ 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

**56. Методика контроля эффективности защиты выделенных помещений при использовании систем виброакустической маскировки.**

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 абсорбционных глушителей. • 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.

**57.Методы выявления электронных устройств негласного получения информации, внедренных в выделенные помещения и технические средства.**

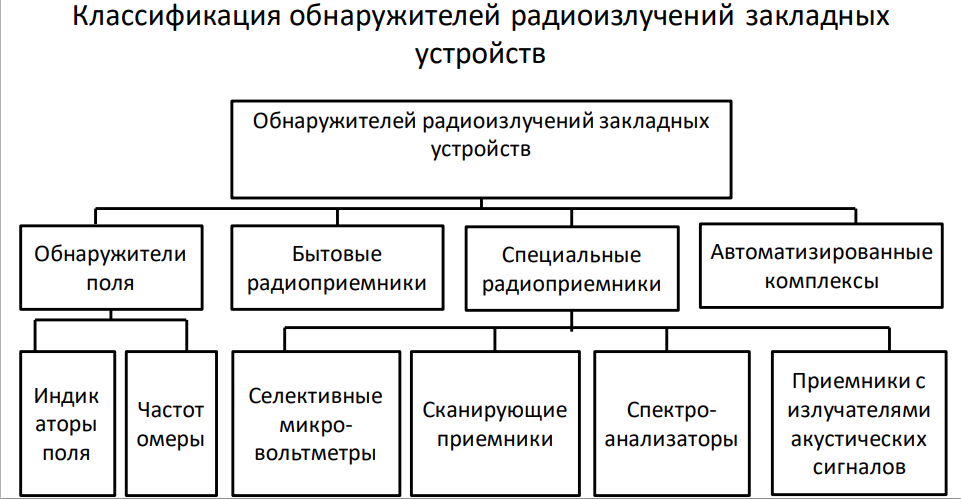
**58. Порядок проверки технических средств и выделенных помещений на наличие электронных устройств негласного получения информации**

**59. Средства выявления электронных устройств негласного получения информации: индикаторы электромагнитного поля**

Простейшими обнаружителями радиоизлучений закладных 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 - частотомеры обеспечивают измерение частоты колебаний поля. Но чувствительность обнаружителей поля мала, поэтому с их помощью можно обнаруживать поля радиозакладок в непосредственной близости от источника излучения.

**60. Средства выявления электронных устройств негласного получения информации: программно-аппаратные комплексы радиоконтроля,**

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. Учитывая, что радиоизлучающие закладки преобладают на рынке закладных устройств, существуют разнообразные средства радиоконтроля обследуемых помещений: от простейших индикаторов электромагнитного поля до сложных автоматизированных комплексов.



Простейшими обнаружителями радиоизлучений закладных 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 - частотомеры обеспечивают 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 (AM 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.

**61. Средства выявления электронных устройств негласного получения информации: анализаторы проводных коммуникаций**

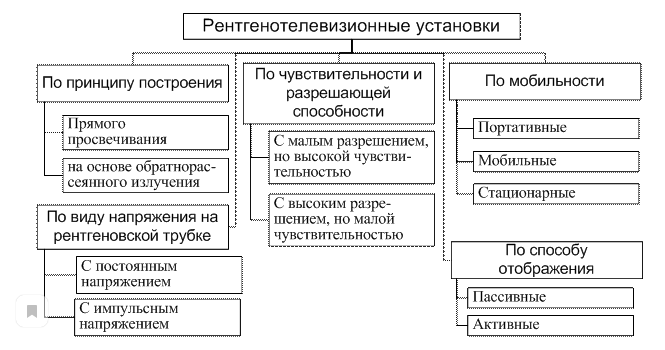
Аппаратура для контроля проводных линий предназначена для выявления в них опасных сигналов и их источников, в том числе закладных устройств. Так как основными направляющими линиями, по которым передаются от закладных устройств электрические сигналы с информацией, являются телефонные линии и цепи электропитания, то соответствующие средства контроля включают приборы контроля телефонных линий и линий электропитания.

**62. Средства выявления электронных устройств негласного получения информации: нелинейные локаторы**

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.

**63. Средства выявления электронных устройств негласного получения информации: рентгено-телевизионные комплексы**

Рентгенотелевизионные установки позволяют в режиме реального времени рассмотреть внутреннюю структуру контролируемого объекта, идентифицировать инородные включения или дефекты. Возможности рентгенотелевизионных систем позволяют обнаружить отдельные элементы оружия и взрывных устройств, контейнеры с опасными вложениями и другие запрещенные к провозу предметы.



Способность рентгеновского излучения проникать через объекты, по разному поглощаясь различными веществами, используется в установках прямого просвечивания. Типовая рентгеноскопическая установка прямого просвечивания состоит из [рентгеновской трубки](https://studopedia.ru/9_40257_rentgenovskie-trubki.html) (излучателя), создающей излучение, преобразователя теневого изображения, блока обработки и визуализации. Исследуемый объект помещается между излучателем и преобразователем. Проходя через него рентгеновские лучи теряют часть своей энергии и попадают на экран преобразователя. Интенсивность лучей в различных областях экрана будет различной и зависеть от веществ, из которых состоит объект исследования. Таким образом, исследуемый объект отбрасывает «тень» на экран преобразователя. Экран преобразователя состоит из флюоросцентных вещества. Воздействие на него рентгеновских лучей вызывает свечения, причем яркость свечения зависит от энергии воздействующего излучения.

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.

**64. Разработка системы защиты информации от утечки по техническим каналам**

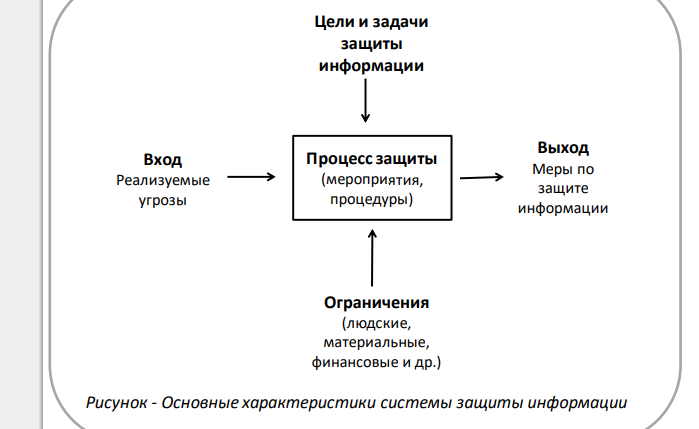
Способы и средства технической защиты информации применяются для создания системы защиты информации, препятствующей реализации угроз утечки информации по техническим каналам. В настоящее время проблема защиты информации относится к числу сложных, слабоформализуемых задач, решаемых на основе системного 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 – 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

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.

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 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;

• 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 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 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 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.

Последовательность проектирования (модернизации) системы защиты включает три основных этапа:

• моделирование объектов защиты;

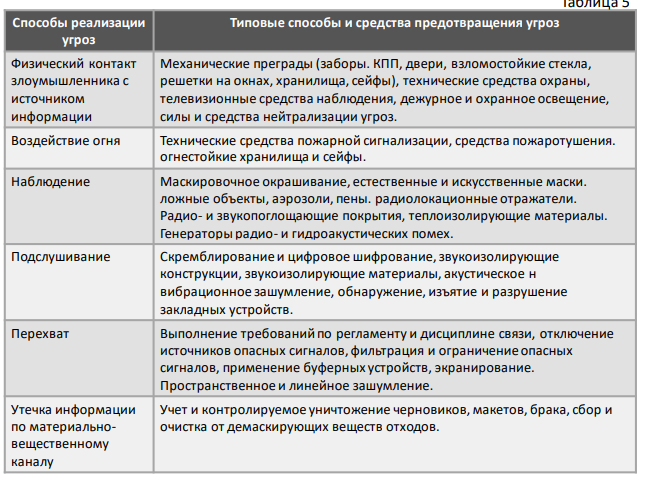
• моделирование угроз информации;

• 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.

**65. Рекомендации по выбору методов и средств защиты информации от утечки по техническим каналам**

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 из таблиц 1 и 3. Следовательно, разработка мер по предотвращению угроз представляет 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. Рекомендуемые способы и средства защиты информации заносятся в таблицу.

Совокупность рассмотренных таблиц, 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.