Краснодарский университет МВД России

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Учебное пособие

Краснодар
2023

УДК 004.056.5
ББК 16.8
Т382

Одобрено
редакционно-издательским советом
Краснодарского университета
МВД России

Составители: *А. В. Еськов, А. С. Победа*

Рецензенты:
В. Э. Баумтрог, кандидат физико-математических наук наук, доцент (Барнаульский юридический институт МВД России);
И. И. Бердинских (Тюменский институт повышения квалификации сотрудников МВД России).

Техническая защита информации : учебное пособие / сост.: А. В. Еськов, А. С. Победа. – Краснодар : Краснодарский университет МВД России, 2023. – 70 с.

Т382

ISBN 978-5-9266-1917-8

Рассматриваются принципы работы технических средств защиты информации и средств поиска устройств съема информации с технических каналов связи. Приводятся характеристики технических каналов связи.

Для профессорско-преподавательского состава, адъюнктов, курсантов, слушателей образовательных организаций МВД России и сотрудников органов внутренних дел Российской Федерации.

УДК 004.056.5
ББК 16.8

ISBN 978-5-9266-1917-8

Предисловие

Информация является одним из важнейших факторов развития современного общества в различных сферах: экономике, финансах, законодательстве, культуре, обороне и безопасности государства. В связи с увеличением угроз безопасности в последнее десятилетие все большую актуальность приобретает состояние защиты информации в целом и технической защиты информации в частности.

Учебное пособие делится на три части: первый пункт – «Методы и средства защиты проводных каналов передачи информации»; второй – «Методы и средства защиты информации от утечки за счет побочных электромагнитных излучений и наводок»; третий – «Технический контроль эффективности мер защиты информации» (в краткой форме содержит основные сведения по основам технической защиты информации). В пособии рассматриваются физические основы принципов действия наиболее часто применяемых технических средств, описана классификация и приведены примеры устройств, используемых в органах внутренних дел для технической защиты информации.

Учебное пособие предназначено для курсантов и слушателей, обучающихся по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере, и может использоваться курсантами, слушателями и адъюнктами при подготовке научных сообщений и для углубленного изучения дисциплины «Физика» и тем, касающихся защиты информации, а также дисциплин «Специальная техника ОВД» и «Техническая защита информации».

1. Методы и средства защиты проводных каналов передачи информации

1.1. Понятие и классификация технических каналов утечки информации

При рассмотрении образования каналов утечки информации наибольший интерес представляют основные технические средства приема, обработки и хранения информации и вспомогательные технические средства и системы.

Посторонние проводники, воспринимающие побочные электромагнитные излучения, являются случайными антеннами. К сосредоточенной случайной антенне относят технические средства с сосредоточенными параметрами, например радиоприемник. Проводники с распределенными параметрами образуют распределенные случайные антенны: интерфейсы, трубы.

Информационные сигналы распространяются в определенных физических средах: твердые, жидкие и газовые. Исходя из природы информационных сигналов и среды их распространения определяются характеристики технических каналов.

Наиболее распространенным каналом утечки информации является электромагнитный, возникающий за счет различного вида побочных электромагнитных излучений и наводок (ПЭМИН). В линиях связи носителем информации является переменное электромагнитное поле, где параметрами волнового процесса являются: амплитуда, частота, фаза и т. п. Электромагнитные излучения средств радиосвязи могут пе-

рехватываться средствами контроля, например каналами конвенциональной радиосвязи, Wi-Fi, Bluetooth.

Наиболее доступная информация, передаваемая путем ПЭМИН, – это данные, вводимые с клавиатуры компьютера или отображаемые на мониторе и передаваемые по соединительному кабелю к системному блоку персонального компьютера. Компьютеры и компьютерные системы порождают электромагнитные излучения, которые являются помехами для радиосвязи и образуют электромагнитный канал утечки информации.

Подобно происходит утечка информации при взаимных наводках сигналов между параллельно проложенными проводниками. Утечка информации в каналах электросвязи возможна путем непосредственного подключения к соединительным линиям.

Канал утечки информации включает в себя источник, среду распространения и приемник информации. Структура канала передачи информации приведена на рис. 1.

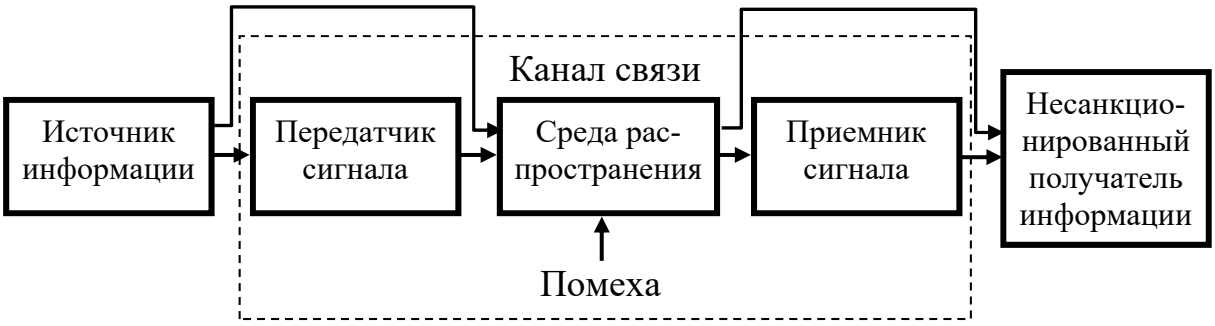


Рис. 1. Структура технического канала утечки информации

Информация от источника поступает на вход канала в формате источника, передатчик преобразует поступающую информацию в формат, соответствующий ее записи на носителе информации и среде распространения.

Среда распространения – часть окружающего пространства, в которой перемещается носитель информации (сигнал).

Приемник выбирает нужный сигнал, осуществляет преобразование информации в формат, доступный получателю.

1.2. Утечка информации при передаче ее по проводным каналам связи

Проводные каналы связи разделяют на витую пару, коаксиальные, оптоволоконные.

Кабель на основе витых пар – это несколько пар скрученных попарно изолированных проводов, объединенных в единую оболочку.

Коаксиальный кабель – это электрический кабель, состоящий из центрального провода и металлической оплетки.

Вследствие того, что электромагнитное поле экранировано внешним проводом, внешнее электромагнитное поле практически не проникает внутрь провода.

Между двумя проводниками с переменным электрическим током, находящимися на определенном расстоянии друг от друга, возникает электромагнитное взаимодействие. Это взаимодействие называется наводками, которые не предусмотрены схемотехническими решениями.

Съем информации, передаваемой по проводным линиям связи, осуществляется с использованием электронных устройств, подключаемых к линиям параллельно, т. е. одновременно к двум проводам (рис. 2, а), последовательно, т. е. в разрыв одного из проводов (рис. 2, б), и с использованием индукционного датчика, т. е. посредством бесконтактного подключения (рис. 3).

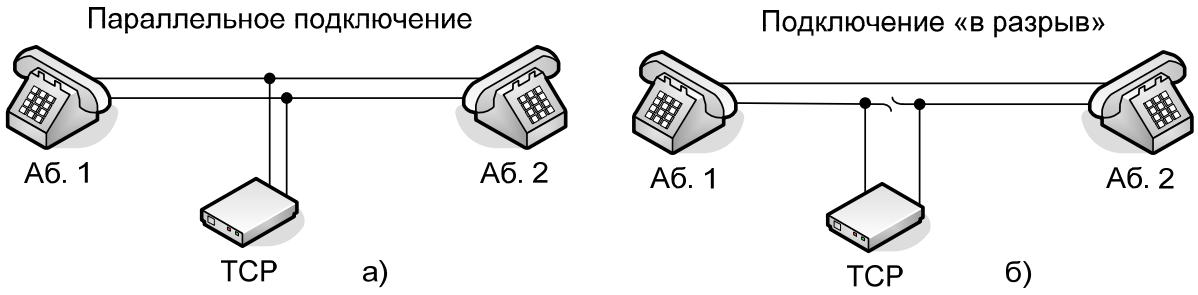


Рис. 2. Подключение закладного устройства к линии связи

Схема параллельного соединения закладного устройства и телефонного аппарата (сопротивлений) изображена на рис. 2, а.

Составим уравнение по первому правилу Кирхгофа:

$$-i + i_1 + i_2 = 0 \text{ или } i = i_1 + i_2 .$$

Поскольку напряжение на любом элементе при параллельном соединении одинаково, то ток в любой ветви на основании закона Ома равен

$$i_K = \frac{U}{R_K} .$$

Подставляя в исходную формулу вместо токов соответствующие им выражения, получаем

$$\frac{U}{R_Э} = \frac{U}{R_1} + \frac{U}{R_2} ,$$

где $R_Э$ – эквивалентное сопротивление всех параллельно соединенных сопротивлений.

Сократив на общий множитель U, имеем

$$\frac{1}{R_Э} = \frac{1}{R_1} + \frac{1}{R_2} .$$

В последнем выражении приведем правую часть к общему знаменателю

$$\frac{1}{R_Э} = \frac{R_1 + R_2}{R_1 \cdot R_2} .$$

Определим $R_Э$:

$$R_Э = \frac{R_1 \cdot R_2}{R_1 + R_2}.$$

Эквивалентное сопротивление по величине меньше любого из сопротивлений, входящих в параллельное соединение.

Учитывая, что при параллельном соединении напряжение на элементах одинаково, формулу можно записать так:

$$i_1 R_1 = i_2 R_2 = i R_Э.$$

Токи в параллельных ветвях распределяются обратно пропорционально сопротивлениям ветвей.

В качестве вывода проведенных рассуждений можно отметить, что при вероятном параллельном соединении закладного устройства с телефонным аппаратом целесообразно контролировать ток в линии связи.

Схема последовательного соединения закладного устройства и телефонного аппарата (сопротивлений) имеет вид, представленный на рис. 2, б. Составим уравнение напряжений по второму правилу Кирхгофа:

$$U - U_1 - U_2 = 0 \text{ или } U = U_1 + U_2.$$

Поскольку через все элементы протекает один и тот же ток, то напряжение на любом элементе, в соответствии с законом Ома, равно

$$U_K = i U_K.$$

Подставляя в исходную формулу вместо напряжений соответствующие им выражения, получаем

$$i R_Э = i R_1 + i R_2,$$

где $R_Э$ – эквивалентное (общее) сопротивление всех последовательно соединенных сопротивлений. Сократив на общий множитель i, имеем

$$R_Э = R_1 + R_2.$$

Отсюда можно сделать вывод о свойстве последовательного соединения сопротивлений. Эквивалентное сопротивление последовательно соединенных активных сопротивлений равно сумме всех активных сопротивлений данной электрической цепи. В соответствии с законом Ома имеем

$$\frac{U_1}{R_1} = \frac{U_2}{R_2} \text{ или } \frac{U_1}{U_2} = \frac{R_1}{R_2}.$$

Это позволяет сформулировать еще одно свойство последовательного соединения сопротивлений: при последовательном соединении активных сопротивлений падение напряжения на каждом сопротивлении прямо пропорционально величине сопротивления, иными словами, на большем сопротивлении будет большее падение напряжения.

В качестве вывода проведенных рассуждений можно отметить, что самым простым является контактное подключение, что вызывает существенное падение напряжения в линии.

Если вблизи телефонной линии расположить индуктивный датчик (рис. 3), то в нем будет наводиться ЭДС, значение которой определяется мощностью передаваемого по линии сигнала.

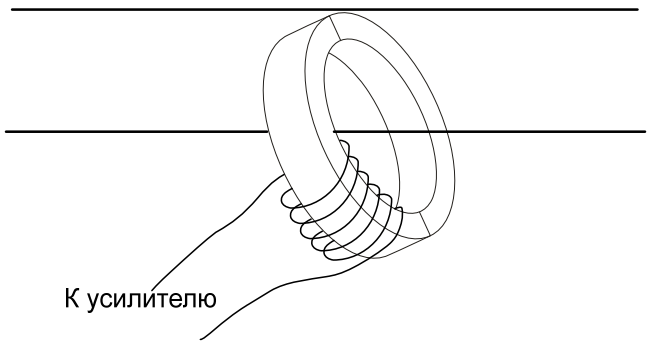


Рис. 3. Подключение к линии индуктивного датчика

1.3. Технические каналы утечки акустической информации

По принципу преобразования акустического сигнала в электрический микрофоны делятся на электродинамические, электростатические, электромагнитные и релейные.

К техническим средствам добывания информации по акустическому каналу относятся микрофоны.

Микрофоны необходимы для преобразования звукового сигнала в электрический. Основные их характеристики:

– чувствительность к звуковым колебаниям;

– частотная характеристика, или полоса звуковых частот, которую прибор может равномерно преобразовать.

Применяются следующие типы микрофонов:

– электродинамические;

– ленточные;

– конденсаторные;

– пьезоэлектрические.

Конденсаторный микрофон конструктивно представляет собой конденсатор (рис. 4), электроемкость которого меняется из-за колебания чувствительной мембраны под воздействием звука, что приводит к получению электросигнала. Преимуществом конденсаторных микрофонов является их точная и достоверная звукопередача по сравнению, например, с электродинамическими микрофонами, а также они, как правило, имеют меньшие размеры.

Следует отметить, что конденсаторному микрофону необходимо электропитание. Некоторые модификации имеют фантомное питание, т. е. подводимое по проводу, идущему к микрофону.

Принцип работы электретного микрофона похож на принцип работы конденсаторного, но на них обеспечивается постоянное значение электрического заряда мембраны, сохраняющей этот заряд длительное время.

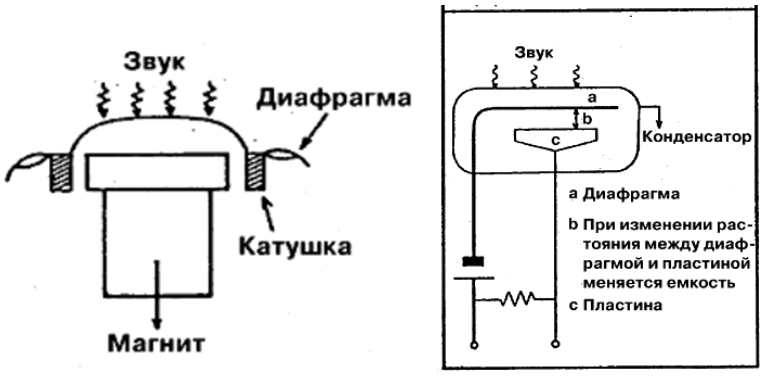


Рис. 4. Устройство электродинамического (слева) и конденсаторного (справа) микрофонов

Электродинамический микрофон представляет собой мембрану, соединенную с легкой катушкой индуктивности, которая помещена в сильное магнитное поле, создаваемое постоянным магнитом. Звуковые колебания воздуха воздействуют на мембрану и приводят в движение катушку. А вибрация катушки в соответствующем магнитном поле приводит к появлению сигнала, пропорционального уровню падающей звуковой волны.

В отличие от конденсаторных, динамические микрофоны не требуют питания, однако они менее чувствительны, чем конденсаторные.

Ленточные микрофоны – это вариант динамического микрофона, содержащего вместо диафрагмы и катушки тонкую гофрированную металлическую ленту, помещаемую в поле магнита. При вибрации ленты под действием звука она начинает действовать как катушка, пусть и с одним витком.

Поскольку лента очень легкая, она обеспечивает значительно более ясный звук, чем обычные динамические микрофоны.

Пьезоэлектрические микрофоны построены на явлении пьезоэффекта, благодаря которому некоторые кристаллы или керамические материалы способны генерировать электросигнал при сообщении им вибрации. Таким образом, материал становится чувствительным к акустическим вибрациям и может выдавать электрическое напряжение в ответ на звук. Пьезоэлектрические микрофоны очень миниатюрны и выдают сигнал менее качественный, чем электродинамические или конденсаторные.

Радиомикрофон представляет собой систему, состоящую из микрофона, переносного малогабаритного передатчика и стационарного приемника. Микрофон чаще всего используют динамический катушечный или электретный. Передатчик либо совмещают в одном корпусе с микрофоном, либо выполняют в карманном варианте. Он излучает радиосигнал в УКВ-диапазоне на одной из фиксированных частот. Вследствие влияния дополнительных преобразований в системе «передатчик – эфир – приемник» качественные параметры радиомикрофона уступают параметрам обычного микрофона.

Направленные микрофоны предназначены, прежде всего, для акустического контроля источников звуков на открытом воздухе.

Для сбора речевой информации из соседнего помещения через стену, потолок, пол используются электронные стетоскопы, регистрирующие акустические колебания в твердых телах.

1.4. Способы контроля проводных линий связи и подавления проводных подслушивающих устройств

Технические средства, предназначенные для контроля проводных линий, используются для обнаружения опасных сигналов и их источников, включая закладные устройства. Главными линиями, по которым передаются электрические сигналы с информацией от закладных устройств, являются телефонные линии и цепи электропитания, поэтому средства контроля проводных линий связи и подавления проводных подслушивающих устройств включают в себя приборы для контроля телефонных линий и линий электропитания.

Способы контроля телефонных линий основаны на изменении электрических параметров линий, вызываемых любым подключением к ним. Это может быть изменение напряжения и тока в линии, значений электроемкости и индуктивности линии, активного и реактивного сопротивления. В зависимости от способа подключения подслушивающего устройства к телефонной линии (последовательного – в разрыв провода телефонного кабеля, параллельного или индуктивного), влияние подключаемого подслушивающего устройства может значительно отличаться, поскольку закладное устройство является активным, величина отбора мощности закладкой из телефонной линии зависит от мощности передатчика закладки и его входного сопротивления. По изменению этих параметров линии возможно выявление закладки при опущенной трубке телефонного аппарата. Контроль линий электропитания осуществляется путем измерения электрических параметров линий, таких как напряжение, ток, активное и реактивное сопротивления. Это позволяет обнаруживать

закладные устройства, которые могут быть подключены к линии электропитания. Помимо телефонных линий и линий электропитания, существуют другие типы проводных линий, которые могут быть подвержены контролю, например: линии передачи данных, линии связи и кабели для передачи видеосигналов. Средства контроля для этих линий могут отличаться от тех, которые используются для телефонных линий и линий электропитания. В целом аппаратура для контроля проводных линий является важным инструментом для обнаружения и предотвращения прослушивания и других форм незаконного доступа к информации, передаваемой по проводным линиям. Она используется в различных отраслях, включая правоохранительные органы, корпоративный сектор и государственные учреждения.

Для контроля телефонных линий применяются следующие устройства:

- устройства оповещения световым и звуковым сигналом об уменьшении напряжения в телефонной линии, вызванном несанкционированным подключением средств подслушивания к телефонной линии;
- измерители характеристик телефонных линий напряжения, тока, емкостного сопротивления и др.), при отклонении которых от установленных норм формируется сигнал тревоги;
- «кабельные радары», позволяющие измерять неоднородности телефонной линии и определять расстояние до неоднородности (асимметрии постоянному току в местах подключения подслушивающих устройств, обрыва, короткого замыкания и др.).

Простейшее устройство контроля телефонных линий представляет собой измеритель напряжения с индикацией конфигурации его значения от обычного, которое фиксируется оператором при работе в режиме настройки путем вращения регулятора на передней панели устройства. Подразумевается, что при настройке номинального напряжения к телефонной линии подслушивающее устройство не подключено. Обычно схожие устройства содержат также фильтры для защиты от прослушивания за счет «микрофонного эффекта» в элементах телефонного аппарата и навязывания на высоких частотах.

Увеличение предельной чувствительности устройств контроля ограничено непостоянностью параметров полосы телефонной линии, колебаниями напряжения источников электропитания на АТС, помехами в линии. Для снижения частоты проявления ошибочных тревог в сложных схожих устройствах наращивают количество измеряемых характеристик телефонной линии, подразумевают возможность накопления и статистической обработки результатов измерений в течение длительного времени линии, находящейся на контроле, а также недалеко расположенных.

Поскольку любое физическое подключение к кабелю телефонной линии создает в ней неоднородность, от которой отражается высылаемый в линию сигнал, то по характеру отражения (амплитуде и фазе) и времени запаздывания отраженного сигнала подсчитывают вид неоднородности и расценивают длину участка линии до неоднородности (места подключения).

Большое количество радиоизлучающих и проводных закладных устройств и методов их использования содействуют

соединению в автоматизированном комплексе средств, реализующих все способы поиска и обнаружения активных закладных устройств. Нельзя не отметить, что в них встраиваются генераторы прицельной помехи, настраиваемой на частоту закладного устройства и подавляющей их сигналы в свободном пространстве и в проводах кабелей. Такая тенденция реализует уменьшение суммарной стоимости средств поиска и обнаружения закладных устройств по их сигнальным признакам и быстроту подавления сигналов в ситуациях, не требующих отлагательств, например во время ответственного совещания, когда нельзя проводить поисковые мероприятия. Для предотвращения гальванического подключения к проводным линиям связи, имеющим небольшую протяженность, их помещают в металлические трубы и ставят под избыточное давление. При попытке подключиться к такому кабелю нарушается герметичность трубы, что вызывает падение давления в ней, о чем выдается сигнал на пульт контроля. Кроме того, производится контроль понижения сопротивления изоляции. При попытке злоумышленника нарушить изоляцию кабеля и получить доступ к проводникам кабеля сигнализатор понижения сопротивления изоляции выдает соответствующий сигнал.

При последовательном либо параллельном гальваническом соединении устройств получения информации их питание реализуется от телефонной линии, при всем этом существуют устройства с компенсацией падения напряжения в телефонной полосе, а при бесконтактном – от автономного источника тока. Приобретенная информация передается, как правило, по радиоканалу.

Радиопередающее устройство активизируется лишь на время телефонного разговора. Не считая того, что устройство

может реализовывать функцию записи речевой информации на магнитный либо использующий другой физический принцип хранения носитель информации. При этом устройство записи активируется исключительно в процессе ведения телефонного разговора. Не исключено прослушивание разговоров методом подключения другого телефонного аппарата в примыкающей комнате.

Рассмотрим методы подавления проводных подслушивающих устройств:

- подача во время разговора в телефонную линию синфазного маскирующего низкочастотного (речевого диапазона) сигнала (метод синфазной низкочастотной маскирующей помехи);
- подача во время разговора в телефонную линию маскирующего высокочастотного сигнала звукового диапазона (метод высокочастотной маскирующей помехи);
- подача во время разговора в телефонную линию маскирующего высокочастотного ультразвукового сигнала (метод ультразвуковой маскирующей помехи);
- поднятие напряжения в телефонной линии во время разговора (метод повышения напряжения);
- подача во время разговора в линию напряжения, компенсирующего постоянную составляющую телефонного сигнала (метод «обнуления»);
- подача в линию при положенной телефонной трубке маскирующего низкочастотного (речевого диапазона) сигнала (метод низкочастотной маскирующей помехи);
- подача в линию при приеме сообщений маскирующего низкочастотного (речевого диапазона) с известным спектром (компенсационный метод);

– подача в телефонную линию высоковольтных импульсов (метод «выжигания»).

Сущность *способа синфазного маскирующего низкочастотного (НЧ) сигнала* (рис. 5) содержится в подаче в каждый провод телефонного кабеля с применением единой системы заземления аппаратуры АТС и нулевого провода электрической сети 220 В (нулевой провод электрической сети заземлен) согласованных по амплитуде и фазе маскирующих сигналов речевого спектра частот (обычно основная мощность помехи располагается в диапазоне частот стандартного телефонного канала от 300 до 3 400 Гц). В телефонном аппарате эти помеховые сигналы компенсируют друг друга и не создают помех воздействию на полезный сигнал (разговор по телефону). В том случае если информация снимается с одного провода телефонной линии, то помеховый сигнал не компенсируется. А поскольку его уровень значительно выше, чем полезный сигнал, то перехват информации (выделение полезного сигнала) не представляется невозможным.

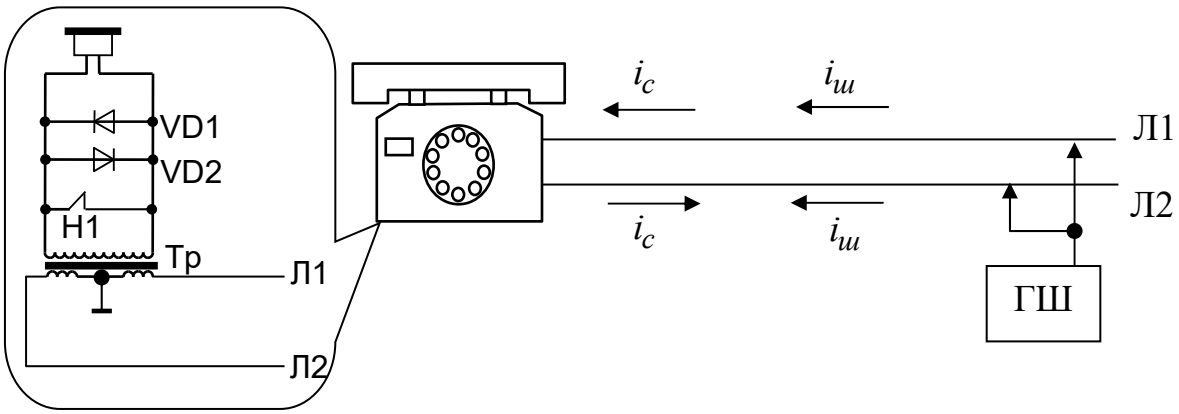


Рис. 5. Принцип метода синфазного маскирующего сигнала

В качестве маскирующего помехового сигнала, как правило, употребляются цифровые сигналы (псевдослучайные последовательности импульсов) речевого спектра частот.

Способ синфазного маскирующего низкочастотного сигнала используется для намеренной поломки телефонных закладок (как с параметрической, так и с кварцевой стабилизацией частоты) с последовательным (в разрыв одного из проводов) включением, а также телефонных радиозакладок и диктофонов с подключением к линии (к одному из проводов) при включении в сеть индукционных датчиков различного типа.

Способ *высокочастотной маскирующей помехи* заключается в подаче на протяжении разговора в телефонную линию широкополосного маскирующего сигнала в диапазоне высших частот звукового спектра (т. е. в спектре высоких частот стандартного телефонного канала). Рассматриваемый способ употребляется для подавления фактически всех видов подслушивающих устройств как контактного (параллельного и последовательного) подключения к линии, так и подключения с использованием индуктивных датчиков. Эффективность угнетения средств съема информации с индуктивных датчиков (особенно не имеющих предусилителей) существенно ниже, чем средств с гальваническим подключением к телефонной полосе.

В качестве маскирующего сигнала употребляются широкополосные аналоговые сигналы типа «белый шум» или цифровые сигналы, состоящие из псевдослучайной последовательности импульсов.

Частоты маскирующих сигналов формируются так, чтобы их уровень оказался достаточным для угнетения полезного сигнала, но при всем этом не снижали качество телефонных разговоров. Чем ниже частота помехи, тем выше ее эффективность и большее помеховое воздействие на необходимый сигнал. В большей степени используются частоты в диапазоне

от 6–8 кГц до 16–20 кГц. Для уменьшения вероятности воздействия маскирующего помехового сигнала на телефонный разговор в устройстве защиты включается в работу особый низкочастотный фильтр с пограничной частотой 3,4 кГц, угнетающий (шунтирующий) помеховые сигналы и не оказывающий большого воздействия на прохождение полезных сигналов.

Способ *ультразвуковой маскирующей помехи* (рис. 6) в основном схож рассмотренному выше. Отличие состоит в том, что используются помеховые сигналы ультразвукового диапазона с частотами от 20–25 кГц до 50–100 кГц.

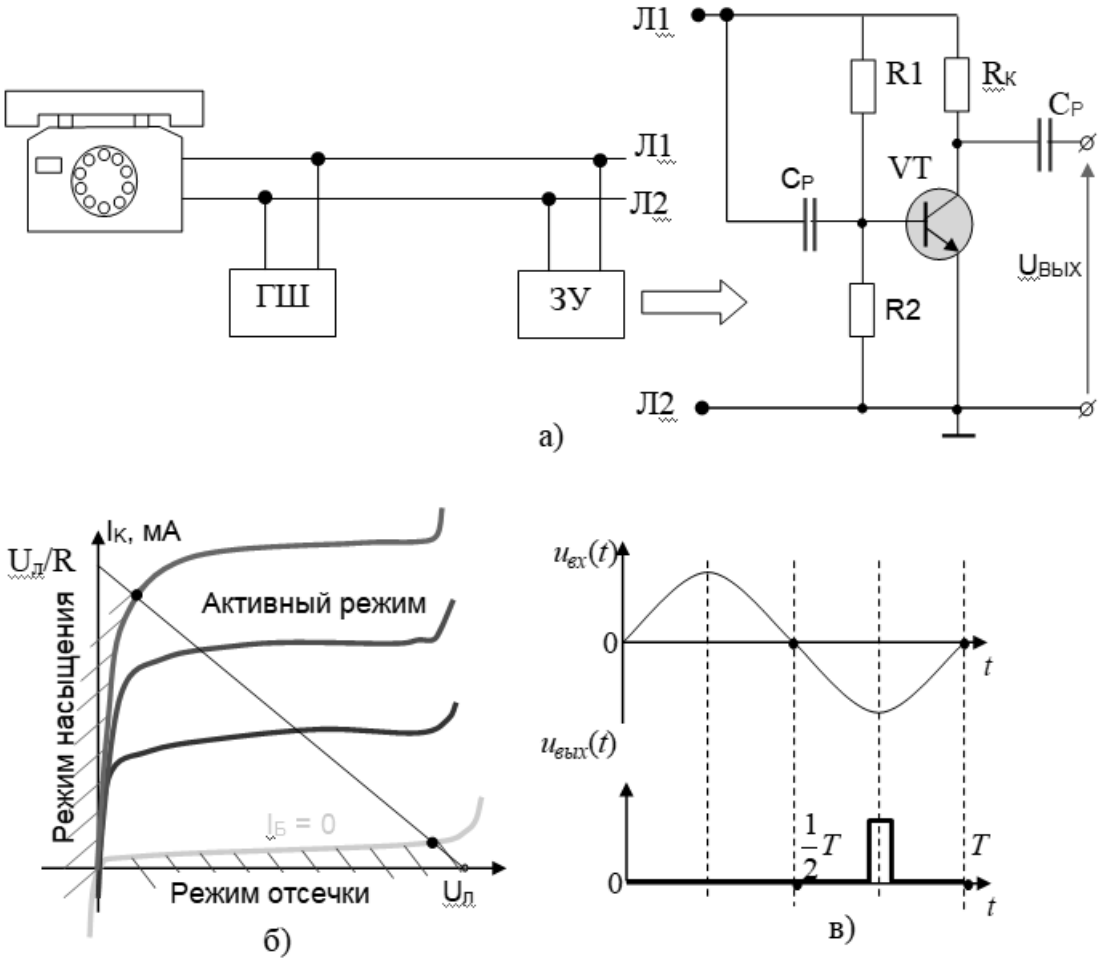


Рис. 6. Принцип ультразвукового подавления

Способ увеличения напряжения состоит в повышении напряжения в телефонной полосе во время разговора и используется для смещения в худшую сторону свойства функционирования телефонных радиозакладок. Увеличение напряжения в линии до 18–24 В влечет у радиозакладок с последовательным подключением и параметрической стабилизацией частоты «уход» несущей частоты и уменьшение разборчивости речи из-за размытия диапазона сигнала. У радиозакладок с последовательным подключением и кварцевой стабилизацией частоты можно проследить ухудшение отношения «сигнал – шум» на 3–10 дБ. Телефонные радиозакладки с параллельным подключением при таких напряжениях в ряде всевозможных случаев просто выйдут из строя.

Способ «обнуления» подразумевает подачу во время разговора в линию постоянного напряжения схожего напряжения в линии при поднятой телефонной трубке, но обратной полярности.

Этот способ употребляется для изменения в худшую сторону функционирования подслушивающих устройств с контактным параллельным подключением к линии, использующих ее в качестве батареи. Этими устройствами являются параллельные стационарные телефоны, проводные микрофонные системы с электретными микрофонами, использующие телефонную линию для передачи информации, акустические и телефонные закладки с питанием от телефонной полосы и т. д.

Способ низкочастотной маскирующей помехи подразумевает подачу в линию при положенной трубке стационарного телефонного аппарата маскирующего сигнала (наиболее часто типа «белый шум») речевого спектра частот (важно,

чтобы основная мощность помехи заключалась в спектре частот обычного телефонного канала от 300 до 3 400 Гц и находила свое применение в подавлении проводных микрофонных систем, использующих телефонную полосу для передачи информации на низкой частоте, а также для ввода в процесс деятельности (включения на запись) диктофонов, подключаемых к телефонной полосе с помощью адаптеров или индукционных датчиков, что приводит к сматыванию пленки в режиме записи шума (другими словами, в случае отсутствия полезного сигнала).

Компенсационный способ (рис. 7) используется для односторонней маскировки (скрытия) сообщений, передаваемых абоненту по телефонной полосе, и имеет в своем функциональном потенциале высокую эффективность подавления известных средств нелегитимного съема информации.

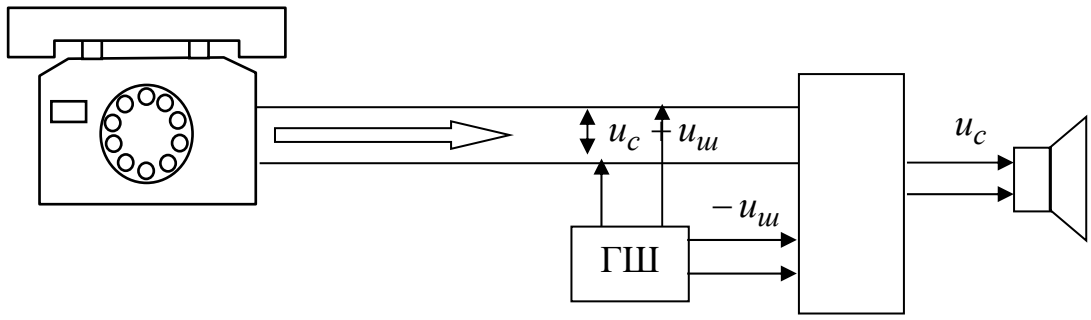


Рис. 7. Принцип компенсационного метода подавления

Сущность метода подразумевает под собой следующее: при передаче тайного сообщения на приемной стороне в телефонный кабель с использованием специального генератора подается маскирующая помеха (дискретный или аналоговый маскирующий сигнал речевого спектра с известным диапазоном). Одновременно этот же маскирующий сигнал («чистый шум») подается на один из входов двухканального адаптив-

ного фильтра, на другой вход которого поступает аддитивная смесь принимаемого полезного сигнала речевого спектра (передаваемого сообщения) и этого же помехового сигнала. Аддитивный фильтр подавляет шумовую составляющую и выделяет полезный сигнал, который подается на телефонное устройство.

Отрицательной чертой рассматриваемого способа является то, что маскировка речевых сообщений односторонняя и не дает возможности вести двухсторонние телефонные разговоры.

Способ «выжигания» осуществляется путем ввода в линию высоковольтных импульсов (напряжением выше, чем 1 500 В), которые приводят к электрическому «выжиганию» каскадов входного типа у электронных устройств перехвата информации и блоков их питания, гальванически подключенных к телефонной полосе.

При использовании рассматриваемого способа аппарат телефонной связи отключается от линии. Подача импульсов в линию производится два раза: первый (для «выжигания» параллельно подключенных устройств) – при разомкнутой телефонной линии, второй (для «выжигания» последовательно подключенных устройств) – при закороченной (как правило, в центральном распределительном щитке здания) телефонной линии.

Способ «выжигания» может привести к полной или частичной неисправности перехватывающих устройств, но не имеет возможности их обнаружения и локализации. Также данный способ может повредить оборудование, подключенное к телефонной линии, которое не имеет отношения к перехвату информации. Поэтому при использовании этого метода

необходимо быть осторожным и убедиться, что все подключенное оборудование соответствует цели проведения «выжигания».

На отечественном рынке имеется большое разнообразие средств защиты. Среди них можно выделить следующие: «SP 17/T», «SI-2001», «КТЛ-3», «КТЛ-400», «Ком-3», «Кзот-06», «Цикада-М», «Прокруст» (ПТЗ-003), «Прокруст-2000», «Консул», «Гром-ЗИ-6», «Протон» и др.

В активных устройствах защиты телефонных линий наиболее часто реализованы метод высокочастотной маскирующей помехи («SP 17/T», «КТЛ-3», «КТЛ-400», «Ком-3», «Прокруст» (ПТЗ-003), «Прокруст-2000», «Гром-ЗИ-6», «Протон» и др.) и метод ультразвуковой маскирующей помехи («Прокруст» (ПТЗ-003), «Гром-ЗИ-6»).

Метод синфазной низкочастотной маскирующей помехи используется в устройстве «Цикада-М», а метод низкочастотной маскирующей помехи – в устройствах «Прокруст», «Протон», «Кзот-06» и др.

Метод «обнуления» применяется, например, в устройстве «Цикада-М», а метод повышения напряжения в линии – в устройстве «Прокруст».

Компенсационный метод маскировки речевых сообщений, передаваемых абоненту по телефонной линии, реализован в изделии «Туман».

Большинство устройств защиты производят автоматическое измерение напряжения в линии и отображают его значение на цифровом индикаторе. В приборе «Гром-ЗИ-6» на цифровом индикаторе отображается уровень уменьшения напряжения в линии.

Для вывода из строя («выжигания» входных каскадов) средств несанкционированного съема информации с гальваническим подключением к телефонной линии используются устройства типа «ПТЛ-1500», «КС-1300», «КС-1303», «Кобра» и т. д.

Приборы используют высоковольтные импульсы напряжением не менее 1 500 – 1 600 В. Мощность «выжигающих» импульсов составляет 15–50 Вт. Так как в схемах закладок применяются миниатюрные низковольтные детали, то высоковольтные импульсы их пробивают и схема закладки выводится из строя.

«Выжигатели» телефонных закладок могут работать как в ручном, так и автоматическом режимах. Время непрерывной работы в автоматическом режиме составляет от 20 с. до 24 ч.

Устройство «КС-1300» оборудовано специальным таймером, позволяющим при работе в автоматическом режиме устанавливать временной интервал подачи импульсов в линию в пределах от 10 мин. до 2 суток.

Вместе со средствами активной защиты в практическом применении часто используются отличные друг от друга устройства, осуществляющие контроль некоторых параметров телефонных полос и позволяющие устанавливать факт нелегитимного соединения с ними.

Способы *контроля телефонных линий* базируются на том, что любое соединение с ними оказывает изменение электрических параметров полосы: амплитуд напряжения и тока в линии, а также значений емкости, индуктивности, активного и реактивного сопротивления линии. В зависимости от метода соединения закладного устройства к телефонной полосе (последовательного, в разрыв одного из проводов телефонного

кабеля или параллельного) степень его влияния на изменение параметров линии будет различной.

Для контроля телефонных линий используются специальные устройства, называемые контрольными телефонными аппаратами (КТА). Существует несколько методов контроля телефонных линий.

1. Амперметрический метод: основан на измерении изменения тока в линии при подключении КТА на него. Этот метод наиболее точен и часто используется при проверке телефонных линий.

2. Вольтметрический метод: основан на измерении изменения напряжения в линии при подключении КТА на него. Этот метод менее точен, поскольку изменение напряжения может быть вызвано не только подключением КТА, но и другими факторами.

3. Импульсный метод: основан на генерации КТА специальных импульсов высокой частоты, которые распространяются по линии и вызывают изменение ее параметров. Этот метод используется реже всего, так как требуется специализированное оборудование и знания.

4. Контроль в разрыве: основан на подключении КТА в разрыв одного из проводов телефонного кабеля. Этот метод используется, когда невозможно подключить КТА в параллель к линии, но его точность низкая.

5. Параллельный метод: основан на подключении КТА параллельно телефонной линии. Этот метод является наиболее простым, но его точность также низкая.

При выборе метода контроля телефонных линий необходимо учитывать их особенности и требования к точности измерений.

За исключением особо важных объектов, линии связи основываются по единому образцу. Ввод линии в здание осуществляется магистральным многопарным (многожильным) телефонным кабелем до внутреннего распределительного щита. Далее от щита до каждого абонента производится разводка двухпроводным телефонным проводом марки ТРП или ТРВ. В статическом режиме любая двухпроводная линия характеризуется волновым сопротивлением, которое определяется погонными емкостью (пФ/м) и индуктивностью (Гн/м) линии. Волновое сопротивление магистрального кабеля лежит в пределах от 130 до 160 Ом для каждой пары, а для проводов марки ТРП и ТРВ имеет место разброс от 220 до 320 Ом.

Существует несколько уязвимых мест, касающихся подключения телефонных линий, которые могут быть использованы злоумышленниками для получения несанкционированного доступа к информации. Эти места включают входной распределительный щит, внутренние распределительные колодки и открытые участки провода ТРП, а также телефонные розетки и аппараты. Наличие современных внутренних мини-АТС не означает, что эти места защищены от атак.

Существует простое устройство контроля телефонных линий, которое может помочь обнаружить подключение посторонних устройств к линии. Это устройство измеряет напряжение на линии и устанавливает порог тревоги. Если напряжение на линии уменьшается ниже установленного порога, устройство подает звуковой или световой сигнал тревоги.

Существуют также устройства, которые сигнализируют о размыкании телефонной линии, которое может быть вызвано подключением закладного устройства. Эти устройства также могут содержать фильтры для защиты от прослушивания

за счет «микрофонного эффекта» в элементах телефонного аппарата и высокочастотного «навязывания».

Однако устройства контроля телефонных линий не всегда являются эффективными в защите от атак. Они могут реагировать на изменения напряжения, вызванные не только подключением к линии средств съема информации, но и колебаниями напряжения на АТС, что приводит к частым ложным срабатываниям сигнализирующих устройств. Поэтому, хотя эти устройства могут помочь обнаружить подключение посторонних устройств к телефонной линии, они не являются панацеей в защите от атак. Важно помнить, что лучшей защитой от атак на телефонные линии является использование криптографических методов шифрования, таких как VPN или шифрование конечного устройства. Эти методы могут обеспечить безопасность передачи данных по телефонной линии и защитить их от несанкционированного доступа.

Принцип работы более сложных устройств основан на периодическом измерении и анализе нескольких параметров линии (напряжения, тока, а также активного и реактивного сопротивления линии). Такие устройства позволяют определить не только факт подключения к линии средств съема информации, но и способ подключения (последовательное или параллельное). Например, контроллеры телефонных линий «КТЛ-2», «КТЛ-3» (см. рис. 7) и «КТЛ-400» за 4 мин. позволяют обнаружить закладки с питанием от телефонной линии независимо от способа, места и времени их подключения, а также параметров линии и напряжения АТС. Приборы также выдают световой сигнал тревоги при кратковременном (не менее 2 с.) размыкания линии. Современные контроллеры телефонных линий, как правило, оборудованы и средствами

их подавления. Для подавления в основном используется метод высокочастотной маскирующей помехи. Режим подавления включается автоматически или оператором при обнаружении факта несанкционированного подключения к линии.

Для блокировки работы (набора номера) несанкционированно подключенных параллельных телефонных аппаратов используются специальные электронные блокираторы. Принцип их работы поясним на примере изделия «Рубин». В дежурном режиме устройство анализирует состояние телефонной линии путем сравнения напряжения в линии и на эталонной нагрузке, подключенной к цепи телефонного аппарата. При поднятии трубки несанкционированно подключенного параллельного телефонного аппарата напряжение в линии уменьшается, что фиксируется устройством защиты. Если это происходит в момент ведения телефонного разговора, срабатывает звуковая и световая (загорается светодиод несанкционированного подключения к линии) сигнализация. А если факт несанкционированного подключения к линии зафиксирован в отсутствие телефонного разговора (трубка на защищаемом телефонном аппарате не снята), то срабатывает сигнализация и устройство защиты переходит в режим блокирования набора номера с параллельного телефонного аппарата. В этом режиме устройство защиты шунтирует телефонную линию сопротивлением 600 Ом (имитируя снятие трубки на защищаемом телефонном аппарате), что полностью исключает возможность набора номера с параллельного телефонного аппарата. Кроме несанкционированного подключения к линии параллельного телефонного аппарата устройство защиты «Рубин» сигнализирует также о фактах обрыва (размыкания) и короткого замыкания телефонной линии.

Контрольные вопросы

1. Какая структура каналов утечки информации?

2. Как классифицируются каналы утечки информации по физической природе носителя?

3. Как классифицируются радиоэлектронные каналы утечки информации?

4. Из-за чего возникают побочные электромагнитные излучения и наводки?

5. Как классифицируются акустические каналы утечки информации?

6. Охарактеризуйте визуально-оптический канал утечки информации.

7. Назовите способы и средства защиты информации от утечки по радиоэлектронному каналу.

8. Назовите способы и средства защиты информации от утечки по акустическому каналу.

9. Назовите способы и средства защиты информации от утечки по визуально-оптическому каналу.

10. Расскажите принцип работы прибора видения в темноте.

11. Какие типы микрофонов Вы знаете? Опишите их принцип работы.

2. Методы и средства защиты информации от утечки за счет побочных электромагнитных излучений и наводок

2.1. Защита информации от утечки за счет побочных электромагнитных излучений и наводок

Защита информации – деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Способ защиты информации – порядок и правила реализации определенных принципов и средств защиты информации.

Техническое средство защиты информации – это комплекс программных и аппаратных средств, предназначенных для установления уровня защиты информации по определенным критериям безопасности. Такие средства могут обеспечивать защиту от несанкционированного доступа, перехвата, модификации, уничтожения или искажения информации. Примерами технических средств защиты информации являются: брандмауэры, виртуальные частные сети, шифрование данных, антивирусные программы, системы распознавания биометрических данных и др.

Классификация методов защиты представлена на рис. 8.

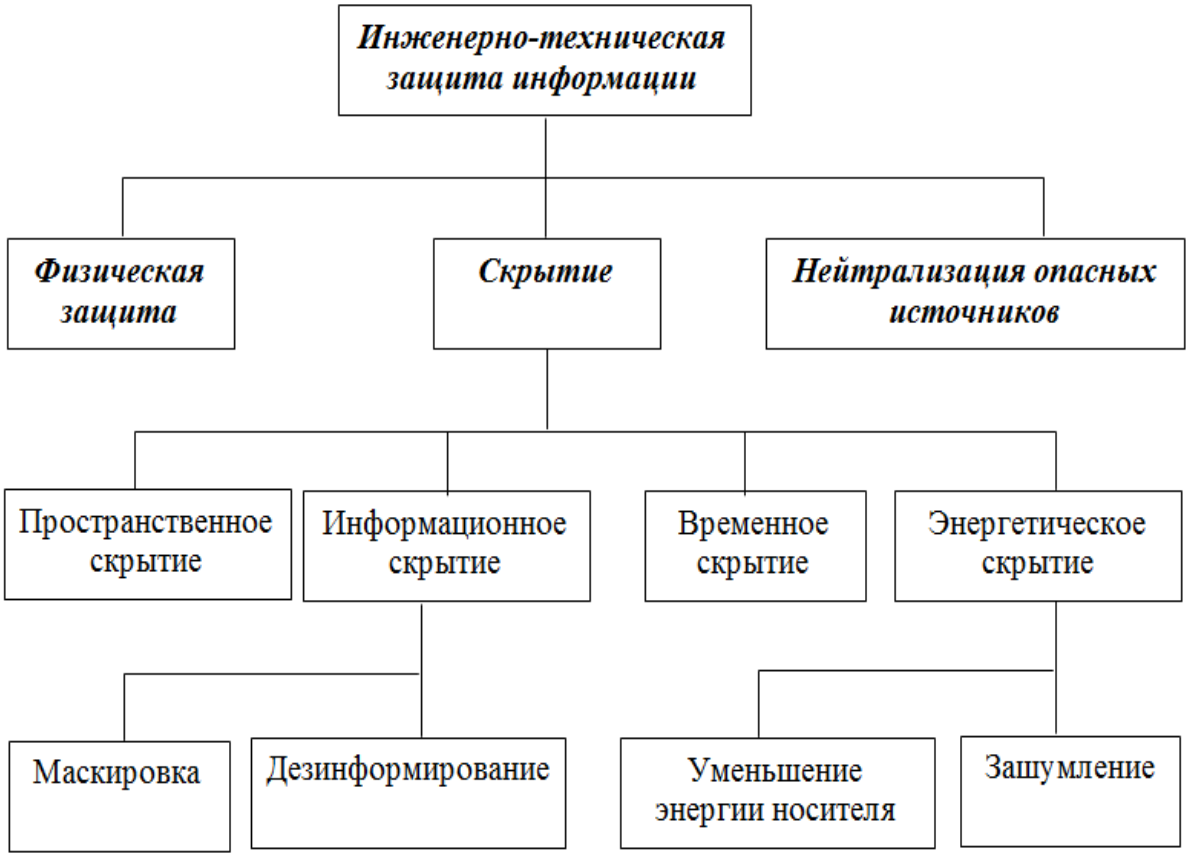


Рис. 8. Классификация направлений и методов ИТЗИ

Способы защиты на основе инженерных конструкций в сочетании с техническими средствами охраны образуют так называемую физическую защиту. Совокупность этих методов, а также соответствующие средства изучаются в рамках курса «Технические средства охраны».

Основные организационные мероприятия по защите информации от утечки за счет побочных электромагнитных излучений представлены на рис. 9.

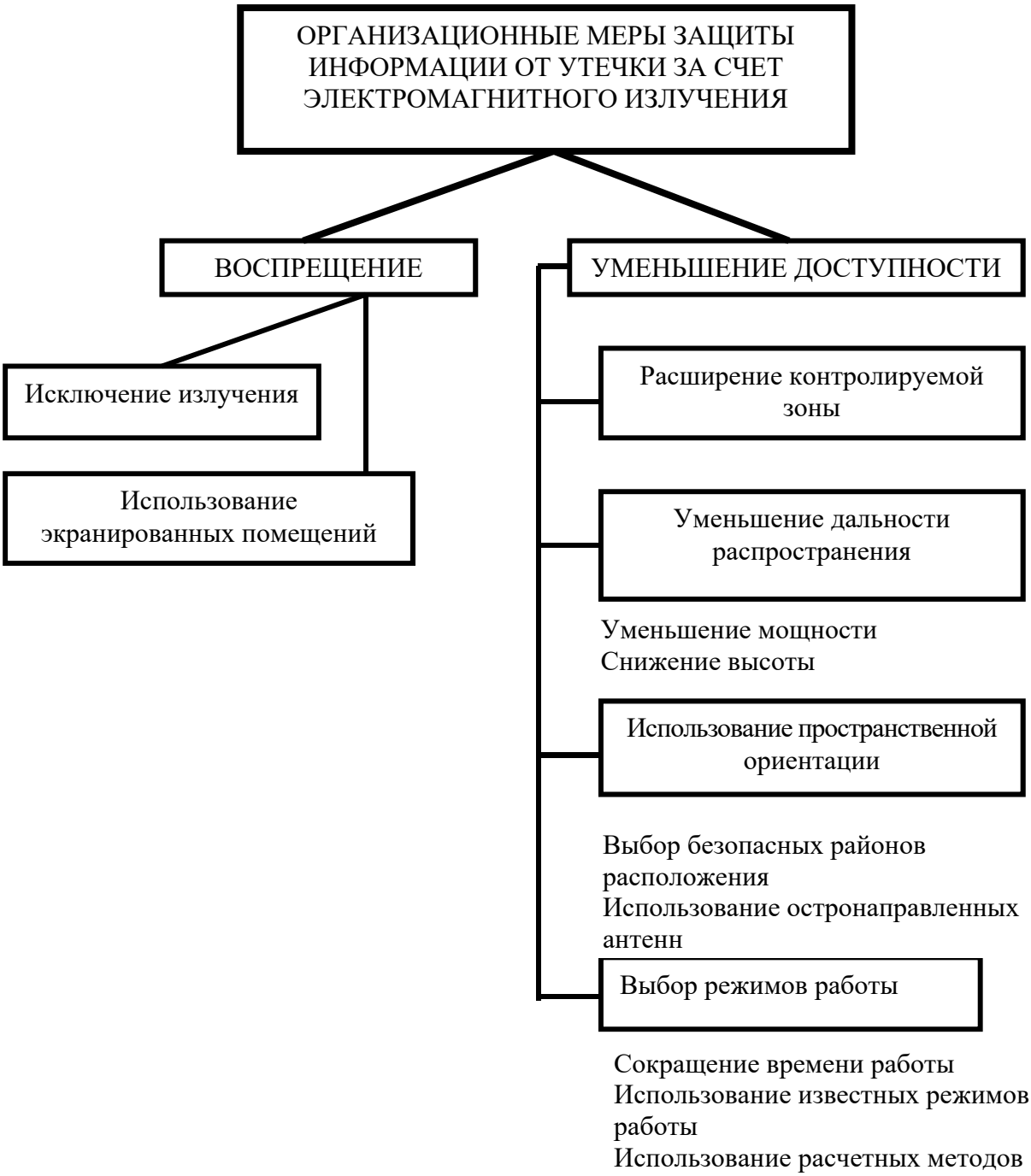


Рис. 9. Организационные меры защиты от утечки информации за счет ПЭМИН

Мероприятия организационной защиты – это совокупность действий организационного характера по защите информации,

проведение которых не требует применения специально разработанных технических средств. Проведение данных мероприятий основывается на характере электромагнитного поля, который изменяется в зависимости от дальности его приема. При этом необходимо рассматривать две области распространения поля: внутри помещения (ближнее поле) и за пределами помещения (дальнее поле). Ближнее поле определяет электромагнитную обстановку в помещении и воздействует путем наведения электромагнитных полей в линиях электропитания, связи и других кабельных магистралях, а дальнее – дальность распространения информационного сигнала в диапазоне радиоволн.

2.2. Пассивные методы защиты от утечки за счет побочных электромагнитных излучений и наводок

Устройства электроники, которые работают с большими напряжениями и малыми токами, создают электромагнитные поля с преобладанием электрической составляющей в ближней зоне. Если элементы электроники малочувствительны к магнитной составляющей, электрические поля оказывают на них наибольшее влияние.

Вместе с тем устройства электроники, которые работают с большими токами и малыми перепадами напряжения, создают электромагнитные поля с преобладанием магнитной составляющей в ближней зоне. Если элементы электроники малочувствительны к электрической составляющей, магнитные поля оказывают на них наибольшее влияние. Кроме того, соединительные линии, такие как провода и кабели, также со-

здают переменные электрические и магнитные поля в пространстве. Побочные электромагнитные излучения от этих соединительных линий могут вызывать электромагнитные и параметрические каналы утечки информации, а также наводки информационных сигналов в посторонних токоведущих линиях и конструкциях. Поэтому снижение уровня побочных электромагнитных излучений является важной задачей.

Электромагнитные поля могут оказывать различное воздействие на элементы электронной аппаратуры. Например, они могут вызывать ошибки в работе устройств, снижать их производительность или даже приводить к поломке. Поэтому проектирование и тестирование электронной аппаратуры должны включать оценку ее устойчивости к электромагнитным полям.

Существуют различные методы для снижения уровня побочных электромагнитных излучений. Например, можно использовать экранирование, чтобы защитить устройства от воздействия электромагнитных полей. Также можно использовать фильтры для снижения уровня шума и помех. Другой метод – это использование материалов с высокой устойчивостью к электромагнитным полям при проектировании устройств. В целом понимание воздействия электромагнитных полей на электронную аппаратуру является важным аспектом проектирования и тестирования устройств. Снижение уровня побочных электромагнитных излучений также является важной задачей, которая может быть решена с помощью различных методов.

Эффективным методом снижения уровня ПЭМИ является экранирование их источников.

Различают следующие способы экранирования:

− электростатическое;

− магнитостатическое;

− электромагнитное.

Электростатическое и магнитостатическое экранирование базируются на покрытии экраном (обладающим в первом случае высокой электропроводностью, а во втором – магнитопроводностью) электрического и магнитного полей соответственно.

Электростатическое экранирование, в частности, приводит к замыканию электростатического поля на внешнюю сторону металлического экрана и отводу электрических зарядов на базу (на корпус прибора). Заземление электростатического экрана является необходимым элементом при реализации электростатического экранирования. Применение металлических экранов позволяет полностью устранить влияние электростатического поля.

Базовой задачей экранирования электрических полей выступает уменьшение емкости связи между экранируемыми элементами конструкции. Можно сделать вывод, что положительная сторона экранирования находит свое проявление в основном отношении емкостной связи между источником и рецептором наводки до и после установки заземленного экрана, ввиду чего любые действия, приводящие к снижению емкости связи, увеличивают эффективность экранирования.

2.3. Активные меры защиты информации от утечки за счет побочных электромагнитных излучений и наводок

В ряде случаев, несмотря на применение пассивных методов защиты, на границе контролируемой зоны отношение «сигнал – шум» превышает допустимое значение. В этом случае применяются активные меры защиты, основанные на создании помех средствам разведки, что также приводит к уменьшению отношения «сигнал – шум».

Под зашумлением понимается создание в местах возможного перехвата сообщений маскирующей помехи с параметрами, исключающими как непосредственное прослушивание сообщений, так и выделение их из помех в результате обработки. Зашумление используют в тех случаях, когда другие организационно-технические меры защиты не закрывают канал утечки информации.

При спецзащите объектов, на которых установлены ТСПИ, следует выбирать оптимальный вариант комплексной (активной и пассивной) защиты, а также учитывать факторы влияния (электромагнитную совместимость) средств активной защиты (САЗ) на качество работы средств обработки информации и других радиоэлектронных средств, расположенных в зоне действия электромагнитных полей средств активной защиты.

Уровень электромагнитного шума, формируемый средствами активной защиты, не должен превышать допустимые уровни на рабочих местах и за пределами объекта, установленные ГОСТом. Основным специальным требованием, предъявляемым к средствам активной защиты, является

обеспечение необходимого уровня маскирующих помех в заданном диапазоне частот.

Эффективность средств активной защиты определяется в ходе аттестационных испытаний объектов, на которых они установлены.

Для того чтобы эффект маскировки при зашумлении был достигнут, необходимо, чтобы сигнал шума удовлетворял определенным требованиям.

1. При зашумлении применяют помехи, спектр которых имеет случайный (шумовой) характер. Помехи подобного рода называются белым шумом.

2. Для эффективной маскировки спектр шума должен перекрывать спектр маскируемого сигнала открытой информации. Например, для зашумления речевых сигналов спектр шума выбирается в 1,5–2 раза шире речевого спектра.

3. Уровень шума должен быть выше уровня маскируемого сигнала открытой информации. Для надежного подавления речевых сигналов уровень шума должен превышать уровень речевого сигнала открытой информации не менее чем в 5–10 раз.

Средства активной защиты делятся на системы линейного зашумления (СЛЗ) и системы пространственного зашумления (СПЗ).

Для исключения перехвата побочных электромагнитных излучений по электромагнитному каналу используется пространственное зашумление, а для исключения съема наводок информационных сигналов с посторонних проводников и соединительных линий – линейное зашумление.

2.4. Линейное зашумление

Системы линейного зашумления применяются при необходимости снижения электромагнитных помех и защиты от перехвата информации в следующих случаях:

- недостаточные уровни переходных затуханий между влияющими и подверженными влиянию кабелями и соединительными линиями;
- воздействие на цепи, провода и устройства вспомогательной аппаратуры низкочастотных электромагнитных полей основной аппаратуры;
- наличие электроакустических преобразований во вспомогательной аппаратуре.

Системы линейного зашумления могут использоваться:

1) в телекоммуникационных системах для защиты передаваемой информации от перехвата и нежелательных помех от электронных устройств;

2) в автомобильных системах связи и управления для предотвращения интерференции и помех от других электронных систем;

3) в системах видеонаблюдения для защиты передающейся видеоинформации от электромагнитных помех;

4) в сетях передачи данных и Интернете для защиты информации от перехвата и защиты от электромагнитных помех и шумов;

5) в системах контроля и управления в промышленности для предотвращения нежелательных электромагнитных воздействий на электронные устройства и системы автоматизации.

Системы линейного зашумления используются в том случае, если не обеспечивается требуемый разнос проводников, выходящих за пределы контролируемой зоны и технических средств обработки информации (т. е. не выполняется требование по зоне 1), однако при этом обеспечивается требование по зоне 2 (т. е. расстояние от ТСПИ до границы контролируемой зоны больше, чем зона 2).

В простейшем случае система линейного зашумления представляет собой генератор шума, формирующий шумовое маскирующее напряжение с заданными спектральными, временными и энергетическими характеристиками, который гальванически подключается в зашумляемую линию (посторонний проводник). На практике подобные системы используются для зашумления линий электропитания. Кроме того, для исключения индуктивного съема информации с кабелей, по которым передается информация, генератор шума может подключаться в свободные пары проводников этих кабелей (рис. 10).

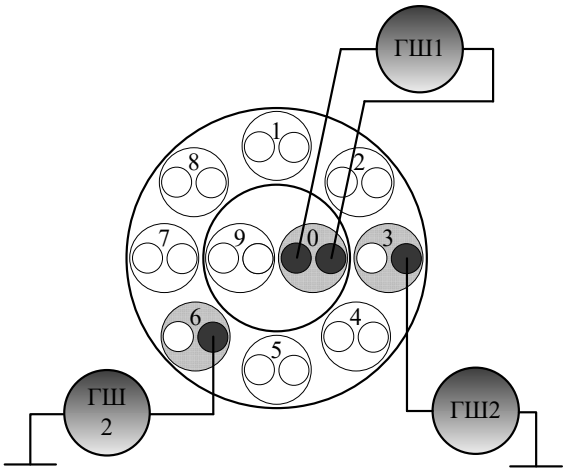


Рис. 10. Вариант подключения генератора шума

В этом случае генератор шума может подключаться к линии по симметричной и несимметричной схемам (рис. 11). По несимметричной схеме генератор шума подключается в центральный повив кабеля (ГШ1 на рис. 10), по несимметричной – во внешний (ГШ2 на рис. 10).

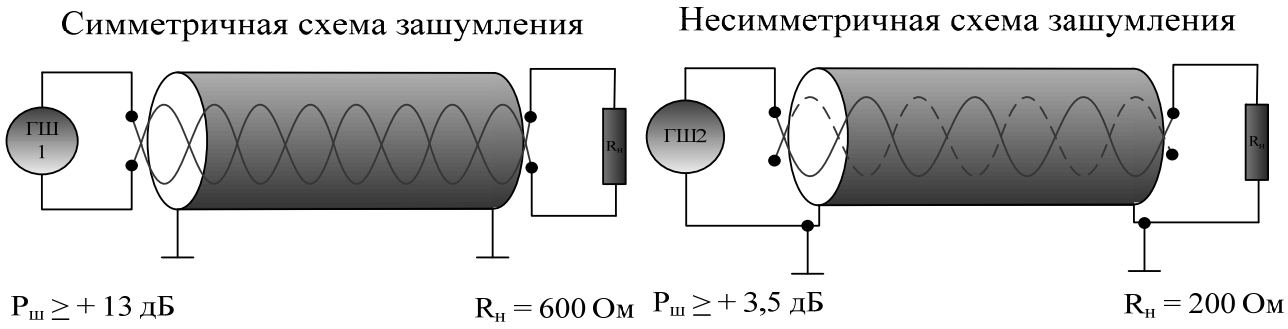


Рис. 11. Несимметричная и симметричная схемы зашумления

2.5. Пространственное зашумление

Системы пространственного электромагнитного зашумления коллективные (СПЗ-К) или индивидуальные (СПЗ-И) применяются для создания маскирующих помех в окружающем ОТСС пространстве.

К системе пространственного зашумления, применяемой для создания маскирующих электромагнитных помех, предъявляются следующие требования:

- генерация электромагнитных помех как с горизонтальной, так и с вертикальной поляризацией в диапазоне частот возможных побочных электромагнитных излучений ТСПИ;
- помехи не должны иметь регулярной структуры;

– уровень создаваемых помех (как по электрической, так и по магнитной составляющей поля) должен обеспечивать отношение «сигнал – шум» на границе контролируемой зоны меньше допустимого значения во всем диапазоне частот возможных побочных электромагнитных излучений ТСПИ;

– на границе контролируемой зоны уровень помех, создаваемых системой пространственного зашумления, не должен превышать требуемых норм по электромагнитной совместимости.

Система магнитных антенн размещается таким образом, чтобы «кабельные петли» находились в трех взаимно перпендикулярных плоскостях. В зависимости от конкретных условий каждая «кабельная петля» может состоять из одного или нескольких полных витков, причем витки могут быть сосредоточены в одной плоскости (образованными отдельными жилами одного кабеля) или в параллельных плоскостях. Прокладка петель выполняется по наружным или внутренним сторонам зашумляемого сооружения (здания).

Выбор количества витков для системы пространственного электромагнитного зашумления коллективной (СПЗ-К) определяется размерами зашумляемого помещения, в котором размещается защищаемое оборудование, и удельной величиной затухания магнитного поля в направлениях, перпендикулярных плоскостям каждой из петель СПЗ-К.

Цель пространственного зашумления считается достигнутой, если отношение «опасный сигнал – шум» на границе контролируемой зоны не превышает допустимого значения, рассчитываемого по специальным методикам для каждой частоты информационного (опасного) побочного электромагнитного излучения ТСПИ. В системах пространственного за-

шумления в основном используются помехи типа «белый шум» или «синфазные помехи».

В системах пространственного зашумления в основном используются слабонаправленные рамочные жесткие и гибкие антенны. Рамочные гибкие антенны выполняются из обычного провода и разворачиваются в двух – трех плоскостях, что обеспечивает формирование помехового сигнала как с вертикальной, так и с горизонтальной полярризацией во всех плоскостях. При вводе в эксплуатацию системы пространственного зашумления необходимо проводить специальные исследования по требованиям обеспечения электромагнитной совместимости (ЭМС).

Контрольные вопросы

1. Назовите классификацию инженерно-технической защиты информации.
2. Что подразумевает под собой скрытие информации?
3. Назовите организационные меры защиты информации от утечки за счет электромагнитного излучения.
4. Что такое воспрещение?
5. Что такое уменьшение?
6. Какие существуют способы экранирования?
7. В каких случаях используются системы линейного зашумления (СЛЗ)?
8. Какие требования выдвигаются к системам пространственного зашумления (СПЗ)?
9. Что такое электростатическое экранирование?
10. Что такое магнитостатическое экранирование?

3. Технический контроль эффективности мер защиты информации

3.1. Контроль характеристик электромагнитного поля

Гармонические колебания – это колебания величины *x,* изменяющейся со временем по закону косинуса либо синуса:

$$x(t) = A\cos(\omega t+\varphi_0), \text{ или } x(t) = A\sin(\omega t+\varphi_0),$$

где $x(t)$ – отклонение величины x от положения равновесия; $\Phi(t) = (\omega t+\varphi_0)$ – аргумент периодической функции (фаза колебания); A – наибольшее отклонение от положения равновесия (амплитуда); φ_0 – начальная фаза; $\omega = 2\pi f$ – круговая, или циклическая, частота; f – частота.

Промежуток времени T, за которое фаза гармонической функции меняется на 2π, является периодом колебания. Действительно, $\Phi(t+T)-\Phi(t) = (\omega(t+T)+\varphi_0)-(\omega t+\varphi_0) = \omega T = 2\pi$. Отсюда получаем $T = 2\pi/\omega$.

Число колебаний в единицу времени – частота: $f = 1/T$. Единица измерения частоты в Международной системе единиц – герц (Гц): 1 Гц = 1 $с^{-1}$, $\omega = 2\pi/\mathrm{T} = 2\pi f$.

Круговая частота ω (циклическая) в 2π раз больше частоты колебаний f; скорость изменения фазы со временем:

$$\frac{d\Phi(t)}{dt} = \frac{d(\omega t + \varphi_0)}{dt} = \omega.$$

При определенной частоте вынужденных колебаний амплитуда достигает максимума. Эта ситуация называется резонансом, а частота $\omega_{\text{рез}}$ – резонансной частотой: $\omega_{рез} = \sqrt{\omega_0^2 - 2\delta^2}$. При $\omega_0^2 < 2\delta^2$ резонанс отсутствует:

$$A_{рез} = \frac{f_0}{2\delta\sqrt{\omega_0^2 - \delta^2}}.$$

Отсюда следует, что при уменьшении коэффициента затухания δ резонансная амплитуда возрастет ($\delta \to 0$, $A_{\text{рез}} \to \infty$) и резонансная частота стремится к частоте незатухающих собственных колебаний ω_0.

Промышленные корпуса, жилые дома, мосты, железные дороги, туннели и прочие объекты являются колебательными системами, в которых возможно возникновение резонанса вплоть до разрушения объекта.

В радиотехнике и электронике резонанс играет очень важную роль. В различных схемах используются резонансные свойства колебательного контура и других резонансных электрических систем. Примером является настройка на нужную частоту передачи радиостанций изменением параметров колебательных контуров.

Пусть сигнал-переносчик – это $X(t)$, а передаваемый сигнал – $B(t)$, тогда модуляция – это преобразование двух сигналов $X(t)$ и $B(t)$ в один модулированный сигнал $U(t)$:

$$U(t) = \mathrm{M}[X(t), B(t)].$$

Для выделения переданного сигнала $B(t)$ из $U(t)$ необходимо выполнить обратное модуляции преобразование – демодуляцию:

$$\mathrm{B(t)} = \mathrm{D}\left[\mathrm{U(t)}\right] = \mathrm{M}^{-1}\left[\mathrm{U(t)}\right].$$

Если под воздействием передаваемого сигнала $B(t)$ информационный параметр сигнала-переносчика $X(t)$ изменяется непрерывно, то все возможные виды модуляции являются непрерывными. К ним относят фазовую, амплитудную и частотную модуляцию и их комбинации.

Самым простым видом модуляции является амплитудно-модулированный (АМ) сигнал (рис. 12). Пусть модулирующий сигнал $u(t)$ является гармоническим колебанием с угловой частотой Ω, амплитудой $U_м$ и начальной фазой, равной нулю:

$$u_м(t) = U_м \cos \Omega t .$$

В качестве несущего (модулируемого) колебания также используется гармоническое колебание с амплитудой $U_н$, некоторой начальной фазой ψ и довольно высокой частотой ω_0:

$$u_н(t) = U_н \cos(\omega_0 t + \psi) .$$

При амплитудной модуляции амплитуда несущего колебания должна изменяться во времени в соответствии с изменениями мгновенного значения модулирующего сигнала $u_м(t)$, т. е. приращение $\Delta U_н(t)$ мгновенного значения огибающей несущего колебания пропорционально приращению $\Delta u_м(t)$ мгновенного значения модулирующего сигнала для любого момента времени *t*:

$$U_н(t) = U_н + a_{AM} U_м \cos \Omega t ,$$

где a_{AM} – коэффициент пропорциональности.

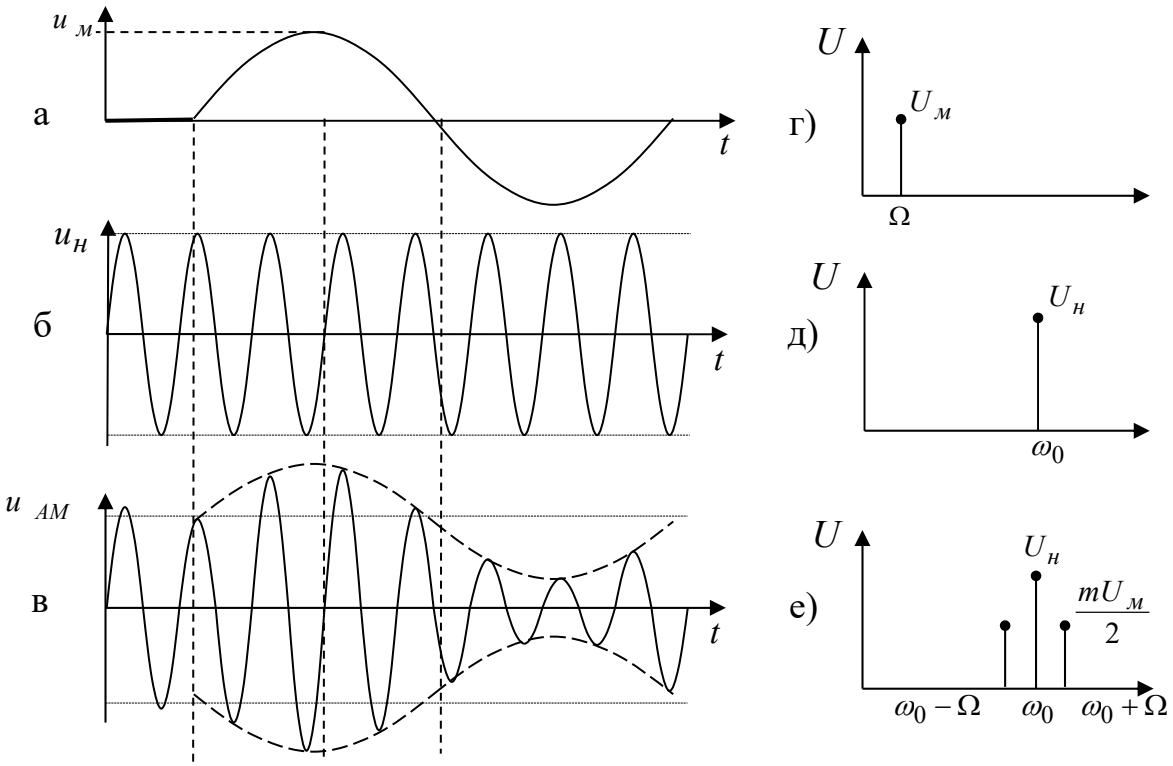


Рис. 12. Сигналы и их спектры при амплитудной модуляции гармонического колебания

Подставляя в последнее выражение вместо $U_н$ из предпоследнего, получим формулу, описывающую АМ-сигнал на любом интервале времени:

$$u_{AM}(t) = (U_н + a_{AM} U_м \cos \omega t) \cos(\omega_0 t + \psi),$$

Следует также рассмотреть соответствующие графики функций (рис. 12, а–в). Огибающая изображена на представленном рисунке штриховой линией.

Произведение $a_{AM} U_м$ – максимальное значение приращения огибающей модулированного сигнала, которое не должно превышать амплитуды модулируемого ВЧ-колебания $u_н(t)$. Используя тригонометрические преобразования, вычислим спектр колебания:

$$u_{AM}(t) = U_н \cos(\omega_0 t + \psi) + \frac{m U_н}{2} \cos[(\omega_0 - \Omega)t + \psi] + \frac{m U_н}{2} \cos[(\omega_0 + \Omega)t + \psi].$$

Таким образом, спектр АМ-сигнала можно рассматривать как сумму трех гармонических колебаний: $u_н(t)$ с амплитудой $U_н$ и частотой ω_0, с амплитудой $mU_н/2$ и частотой $\omega_0 - \Omega$ и, наконец, с амплитудой $mU_н/2$ и частотой $\omega_0 + \Omega$. Примеры спектров модулирующего сигнала, несущего колебания и АМ-сигнала для этого случая приведены на рис. 12, г–е.

Спектр ЧМ-сигнала при $m_ч << 1$ аналогичен спектру АМ-сигнала и также состоит из несущего колебания и двух боковых составляющих с частотами $\omega_0 + \Omega$ и $\omega_0 - \Omega$.

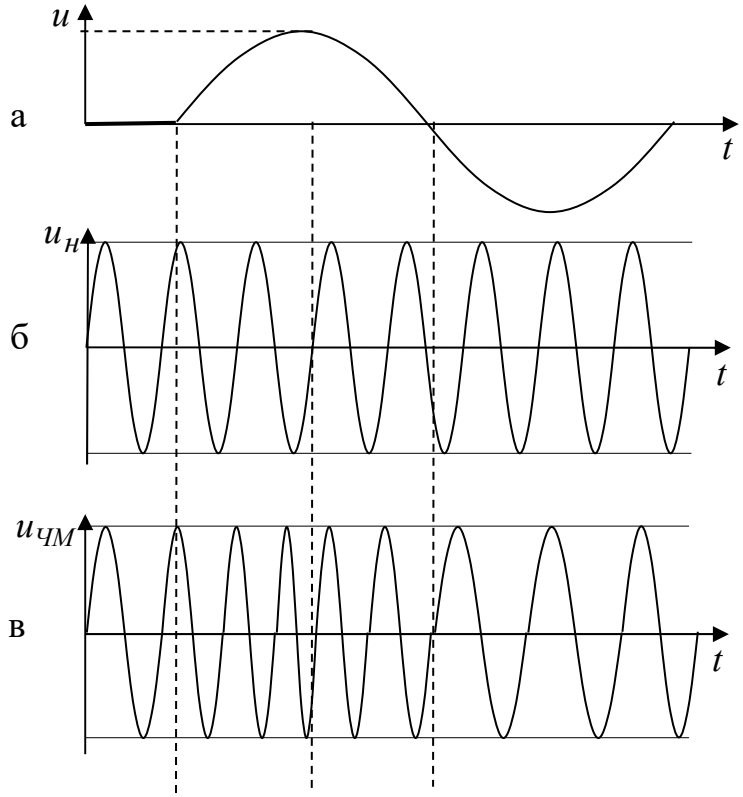


Рис. 13. Частотно-модулированный сигнал

При $m_ц > 1$ спектр ЧМ-сигнала (аналогично и ФМ-сигнала) сложнее и теоретически бесконечен (рис. 13, 14). Считается, что величина спектра радиосигнала с угловой модуляцией

$$\Delta\omega_{уМ} = 2(m+1)\Omega.$$

Следует отметить, что ЧМ- и ФМ-сигналы, применяемые на практике, имеют индекс модуляции $m_ц >> 1$, поэтому

$$\Delta\omega_{уМ} = 2m\Omega.$$

Таким образом, полоса частот, занимаемая сигналами с угловой однотональной модуляцией, значительно шире, чем при амплитудной. Этим объясняется невозможность ее использования на НЧ-, ВЧ- и ВЧ-диапазонах. Угловую модуляцию применяют на ОВЧ и на более коротких волнах.

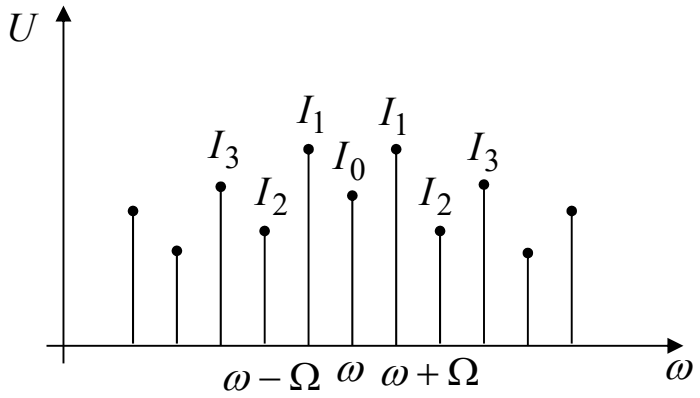


Рис. 14. Спектр частотно-модулированного сигнала

К узкополосной модуляции относятся все виды модуляции AM, FM, PM, формирующие предельно узкий спектр в непосредственной близости от несущей частоты. К широкополосным методам модуляции относятся модуляции с сигналами, имеющими широкий шумоподобный спектр частот, который может быть соизмерим с величиной несущей частоты.

Используются два типа широкополосной модуляции:

– метод прямой последовательности (DSSS);

– метод частотных скачков (FHSS).

Автоматизацией измерения уровней сигналов обладают практически все современные комплексы.

3.2. Способы и средства обнаружения каналов утечки информации

При осуществлении измерений побочных электромагнитных излучений и наводок необходимо получить данные о конфигурациях напряженности поля в близлежащем пространстве или токов и напряжений в некоторых цепях, появляющихся под действием электрических процессов создания

информационных сигналов. Источники полей и наводок не могут быть полностью даны в терминологических справочниках, опубликованных специально для описания простых, эталонных функций времени – синусоидальных колебаний, квазипостоянных величин. При появлении наводки осуществляется, как правило, дальнейшее усложнение формы тока или напряжения, ввиду чего задача выбора системы параметров побочного поля или наводки не является простой и предполагает самостоятельного решения в каждом отдельном случае. Вместе с тем используемые измерительные приборы предназначены для определения общепринятых параметров электромагнитных процессов. Абсолютное большинство измерительных приборов нацелено на обыкновенные составляющие – усредненные значения переменных на интервале времени, причем даже закон усреднения не всегда точно определен.

Задача становится сложной благодаря тому, что для оценки защищенности необходимы не столько энергетические, сколько информационные составляющие процесса. Наиболее перспективным направлением прогрессирования измерительной техники относительно задачи анализа информативности побочных излучений и наводок в низкочастотном диапазоне следует отметить появление измерительных регистраторов электрических величин на базе скоростных АЦП.

Наиболее совершенные приборы общего применения такого типа поставляет на рынок фирма Hewliett Packard. Регистраторы прямой записи имеют разрешение по частоте до десятков мегагерц, а в стробоскопическом режиме – до единиц гигагерц. Разрешение по напряжению составляет единицы милливольт в режиме единичной записи и достигает единиц микровольт в режиме накопления. Регистраторы сопрягаются

по стандартному стыку с ПЭВМ, что позволяет в процессе обработки результатов измерений свободно формировать систему параметров, наиболее адекватно описывающую измеряемые величины.

На современном этапе развития информационных технологий можно проследить тенденцию построения измерительно-вычислительных комплексов на базе ПЭВМ, основанных на адаптерах ввода аналоговых сигналов. В конечном счете получается похожий результат, но если в первом случае прогрессирование идет со стороны измерительного прибора, во втором случае – со стороны ПЭВМ. По состоянию на настоящее время комплексы, основанные на измерительных приборах, имеют большую чувствительность и более широкий частотный диапазон, а для комплексов, имеющих в основе ПЭВМ, характерны многоканальность и развитые пакеты обработки и визуализации сигналов.

Способы и средства обнаружения каналов утечки информации включают в себя:

1) проверку сетевых настроек (может включать проверку конфигурации брандмауэра, настройки доступа к сети, обнаружение несанкционированных точек доступа Wi-Fi);

2) мониторинг событий безопасности (может включать мониторинг аномальной активности или изменений в сети, обнаружение несанкционированных доступов, мониторинг использования несанкционированных устройств);

3) использование специализированного программного обеспечения (может включать использование программных средств для обнаружения сетевых уязвимостей, к которым могут обращаться злоумышленники, обнаружение утечки данных,

мониторинг наличия шпионского или вредоносного программного обеспечения);

4) физический обход (может включать проверку серверных комнат на незакрытые или несанкционированные доступы, обнаружение незаконных использований USB-накопителей, обнаружение использования камеры для захвата конфиденциальной информации и других методов);

5) обучение пользователей (может включать проведение обучения сотрудникам компании о том, какие данные являются конфиденциальными, какие методы могут использоваться злоумышленниками для получения доступа к этим данным и какие меры безопасности могут быть приняты для предотвращения утечки данных).

Использование вышеупомянутых комплексов показывает эффективный результат, если в конфигурации имеется специальное, синхронизированное с АЦП формирование информативных сигналов в рассматриваемом объекте. Используемые в современном мире франшизы генераторов синусоидальных и импульсных сигналов в этом случае несовершенны. Имеющиеся на данном этапе логические анализаторы и формирователи тестовых сигналов обычно создаются для выполнения других задач функционального контроля аппаратуры. По этой причине проблема использования стимулирующего воздействия на рассматриваемый объект – достаточно непростая задача. В комплексах на базе ПЭВМ, сопряженных с АЦП, обычно имеются выходы ЦАП, позволяющие формировать сигналы, воздействующие на объект исследования, но их частотный и амплитудный диапазон, возможности регулировок довольно ограничены.

Рассматриваемые комплексы не полностью отвечают требованиям измерения слабых сигналов при декоммуникации процессов утечки информации из-за отсутствия изоляции между входами сигнала и входами синхронизации. Все указанные недостатки можно преодолеть (основные трудности не выявлены), и есть веские основания полагать, что наиболее перспективными системами измерения являются те, которые работают с представлением сигнала в виде временной последовательности.

В то же время для относительно простых измерений, когда параметры процесса достаточно ясны, неоспоримым преимуществом являются анализаторы спектра и приемники измерений, управляемые персональными компьютерами.

В заключение анализа настоящего состояния аппаратурной базы и прогресса ее развития можно сделать вывод, что для осуществления измерений при оценке каналов утечки на текущий момент важно обратить внимание на измерительно-вычислительные комплексы на базе ПЭВМ, сопряженной с управляемым спектроанализатором НЧ-диапазона и измерительным приемником с частотным диапазоном не менее 2 ГГц, а на перспективу – комплексы на базе скоростных АЦП с полным переносом обработки сигнала в ПЭВМ.

Базовыми компонентами для обоих рассматриваемых случаев являются:

– проблема генераторов стимулирующих воздействий, о которой упоминалось выше;

– проблема входных преобразователей, которая рассматривается в следующем подпункте;

– проблема поверки комплекса в целом, пути решения которой на данный момент неясны.

3.3. Требования, предъявляемые к минимальному набору специальной аппаратуры контроля

В связи с разнообразием средств обнаружения закладок службы безопасности организаций сталкиваются с проблемой выбора и эффективного использования таких устройств.

Можно приобрести различные наборы средств для чистки помещений. Рациональным выбором является приобретение средств, которые окупаются в течение пяти лет, по сравнению с затратами на уборку помещений при арендованных средствах или привлечении специализированных компаний.

В общем случае состав средств для выявления закладок можно разделить на три типа: минимальные, средние и максимально возможные.

Минимальный набор включает:

– фонарь для освещения темных мест при визуальном поиске;

– индикатор поля;

– сканирующий портативный приемник;

– управляющая программа типа Sedif, FIJLIN;

– компьютер, установленный в контролируемом помещении;

– анализатор телефонной линии;

– портативный металлоискатель.

Такой набор обеспечивает:

– визуальный осмотр помещений с освещением и контролем уровня электромагнитного поля в труднодоступных местах;

– обнаружение сканирующим приемником излучений закладок с локализацией мест их установки с помощью индикатора поля;

– обнаружение неизлучающих закладок в плохо проводящей электрический ток среде (кирпичных стенах, мебели, шкафах и т. д.).

Исходя из этого, учитывая, что в выделенных помещениях обычно устанавливают ПЭВМ, целесообразно объединить ее со сканирующим приемником и использовать программу Sedif или более эффективную FIJLIN для автоматизированного анализа радиообстановки в помещении. В этом случае достигается более высокая вероятность обнаружения радиозакладных устройств. Стоимость такого набора (без компьютера) оценивается порядка 50 000 – 75 000 руб., но он не обеспечивает надежного выявления закладных устройств, прежде всего дистанционно управляемых закладок, подключенных к электросети или размещаемых в пустотах железобетонных стен.

Средний набор содержит:

- электрический фонарь;
- досмотровое зеркало;
- индикатор поля;
- частотомер;
- автоматизированный комплекс радиомониторинга помещения;
- анализатор телефонных линий и линий электропитания;
- портативный металлоискатель;
- генератор помех в радиодиапазоне.

Для более высокой вероятности обнаружения закладных устройств рекомендуется использовать комплект максимального

набора, который включает в себя нелинейный локатор вместо металлоискателя. Этот локатор помогает выявлять неизлучающие устройства, находящиеся в труднодоступных и скрытых местах, где другие средства не могут их обнаружить. Для измерения побочных электромагнитных излучений и наводок необходимо определить параметры напряженности поля в окружающем пространстве или токов и напряжений в цепях, которые возникают под действием электрических процессов формирования информационных сигналов. Этот состав обеспечивает более высокую вероятность обнаружения закладных устройств, чем возможность предыдущего варианта за счет радиомониторинга помещения.

В терминах синусоидальных колебаний, которые используются для описания простейших функций времени, невозможно полностью описать источники полей и наводок. Когда возникает наводка, форма тока или напряжения обычно усложняется. Поэтому выбор системы параметров для побочных полей или наводок является сложной задачей, которая требует отдельного решения в каждом конкретном случае. В то же время измерительные приборы предназначены для определения общепринятых параметров электромагнитных процессов. Большинство измерительных приборов ориентированы на простейшие параметры, такие как усредненные значения переменных на определенный интервал времени, но даже закон усреднения не всегда точно определен.

3.4. Нелинейные радиолокаторы

В разнообразном арсенале террористических средств значительное место занимают взрывные устройства, оснащенные радиоуправляемыми детонаторами и (или) взрывателями с электронными таймерами. Традиционным средством поиска таких взрывных устройств при обследовании подозрительных объектов являются металлодетекторы, но они имеют низкую помехоустойчивость в присутствии металлического мусора и малую дальность обнаружения.

Для этой цели предназначены нелинейные радиолокаторы, которые способны обнаруживать электронные и электромеханические взрыватели, радиозакладки и другие радиоэлектронные устройства, даже находящиеся в выключенном состоянии, благодаря своей возможности выявлять радиоэлектронные устройства с нелинейными вольтамперными характеристиками, такие как полупроводниковые элементы, диоды, транзисторы, интегральные микросхемы и т. д.

Для работы нелинейных радиолокаторов необходимо облучать исследуемый объект СВЧ-сигналом, который может быть импульсным или гармоническим. Затем происходит прием переизлученного (отраженного) сигнала на удвоенной и утроенной частотах зондирующего сигнала. Этот сигнал анализируется нелинейным локатором. Функционирование нелинейных радиолокаторов основано на облучении обследуемого объекта СВЧ-сигналом (импульсным или гармоническим) и приеме переизлученного (отраженного) сигнала на удвоенной и утроенной частотах зондирующего сигнала, который анализируется нелинейным локатором (рис. 15).

Существуют материалы, называемые «ложными» полупроводниками, которые также могут иметь эффект нелинейного преобразования зондирующего сигнала. Окисленные металлические элементы и контакты двух разнородных металлов – примеры таких материалов. Однако свойства сигнала, отраженного полупроводниковыми элементами, отличаются от свойств сигнала, отраженного «ложным» полупроводником. Вторая гармоника (удвоенная частота) зондирующего сигнала переизлучается преимущественно полупроводниками, в то время как ложные полупроводники переизлучают утроенную гармонику.

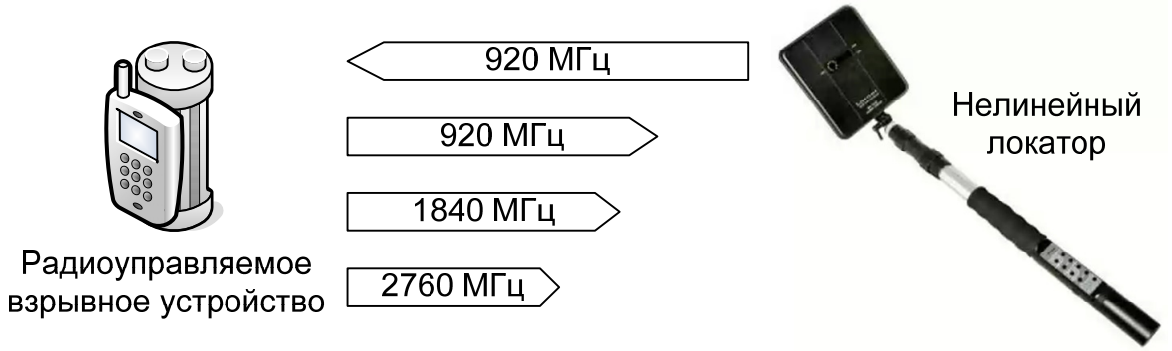


Рис. 15. Принцип нелинейной локации

С помощью современных детекторов нелинейных переходов возможен анализ состава переизлученного сигнала, который позволяет эффективно выделять электронные устройства на фоне других объектов, в том числе и тех, которые имеют схожие свойства.

При обследовании помещения необходимо по возможности убрать приборы, содержащие полупроводниковые элементы. Это необходимо, чтобы исключить ложные срабатывания нелинейного локатора. Перемещать антенный блок

необходимо медленно, параллельно обследуемой поверхности, изменяя ориентацию антенн. Характер изменения принимаемого сигнала оценивается визуально по шкале или на слух по второй и третьей гармоникам. Для более точной локализации полупроводникового элемента необходимо повторить обследование на пониженной мощности. При интенсивном постукивании по исследуемой поверхности показания индикаторов по третьей гармонике, как правило, изменяются.

3.5. Инженерно-техническая укрепленность охраняемых объектов

Обнаружение проникновения злоумышленника в охраняемую зону или возникновение пожара – это основная функция системы охранно-пожарной сигнализации. После обнаружения система передает сигнал тревоги и обеспечивает оперативность действий нарядов, которые прибывают на объект по этому сигналу.

Рассмотрим назначение элементов охранно-пожарной сигнализации.

В состав любой системы охранной сигнализации входят извещатели, приемно-контрольные приборы (ПКП), оповещатели и системы передачи извещений (СПИ).

Охранный извещатель – техническое средство охранной сигнализации, предназначенное для обнаружения проникновения злоумышленника в охраняемую зону и формирования извещения о проникновении.

Извещение о проникновении – сообщение, несущее информацию о проникновении в охраняемую зону и представленное с помощью электрических, световых и (или) звуковых сигналов.

Шлейф сигнализации – электрическая цепь, соединяющая извещатели с приемно-контрольными приборами.

Приемно-контрольный прибор – техническое средство охранной сигнализации, предназначенное для приема извещений от извещателей и передачи их на пульт СПИ и (или) выдачи команд на включение оповещателей.

Оповещатель – техническое средство охранной сигнализации, предназначенное для оповещения людей о проникновении в охраняемую зону путем подачи звуковых и (или) световых сигналов (звонки, ревуны, сирены, обычные или специальные электролампы).

Система передачи извещений – техническая система, осуществляющая контроль за состоянием средств сигнализации, установленных на объектах, прием информации со всех объектов на пункте централизованной охраны (ПЦО) и выдачу дежурному оператору всей необходимой информации о ситуации в зоне его контроля. Извещение может передаваться по линиям ГТС с переключением на период охраны, по занятым линиям ГТС, по радиоканалу.

Технические средства охраны периметра выбираются в зависимости от вида предполагаемой угрозы объекту, помеховой обстановки, рельефа местности, протяженности и технической укрепленности периметра, типа ограждения, наличия дорог вдоль периметра, зоны отторжения, ее ширины.

Извещатели классифицируются по следующим признакам (рис. 16).

1. По форме зоны обнаружения:

− точечные (предназначены для блокирования уязвимых мест (дверей, окон, люков и т. п.) на открывание или отдельных предметов от хищения);

− линейные (предназначены для защиты внутренних и внешних периметров охраняемых объектов);

− поверхностные (предназначены для блокирования определенных поверхностей (окон, дверей), а также тонкостенных строительных перегородок);

− объемные (предназначены для блокирования определенного объема различного типа и назначения помещений и выдающие извещение при перемещении какого-либо предмета или движении человека в данном объеме).

2. По физическому принципу обнаружения:

− контактные: электроконтактные, магнитоконтактные, ударно-контактные, омические (обрывные);

− оптико-электронные: активные, пассивные;

− акустические: звуковые, ультразвуковые;

− вибрационные;

− сейсмические;

− радиоволновые: радиолокационные, радиолучевые, радиотехнические;

− емкостные;

− комбинированные.

Рис. 16. Классификация извещателей

При замыкании или размыкании контактов контактные извещатели срабатывают, обнаруживая действия нарушителей.

Для обнаружения нарушителя и пожара в оптико-электронных извещателях применяются инфракрасные лучи. А для обнаружения нарушителя в акустических извещателях используются акустические волны, которые могут быть как в звуковом, так и в ультразвуковом диапазонах.

К вибрационным относятся извещатели, обнаруживающие нарушителя по создаваемой им вибрации.

Радиоволновые извещатели используют для обнаружения нарушителей электромагнитные волны.

В радиолокационных извещателях используется эффект Доплера. Они выдают сигнал тревоги при приеме отраженного от нарушителя сигнала с измененной частотой. Диапазон

регистрируемой скорости передвижения нарушителя при обнаружении 0,3 – 3 м/с.

Радиотехнические и радиолучевые извещатели обнаруживают нарушителя по изменениям им характеристик СВЧ-поля.

Емкостные извещатели создают сигналы тревоги при приближении нарушителя к антенне.

В качестве чувствительных элементов тепловых извещателей применяются: терморезисторы, термобиметаллические пластины, термоферриты, термоконтактные извещатели.

Ионизационные извещатели реагируют на дым.

3. По способу формирования сигнала от нарушителя:

– активные (излучают определенный сигнал в контролируемую зону);

– пассивные (не излучают никакого сигнала).

4. По устойчивости к воздействию климатических факторов:

– для наружной установки;

– для неотапливаемых и отапливаемых помещений;

– только для отапливаемых помещений.

5. По способу электропитания:

– не потребляющие (пассивные) электроэнергию;

– питающиеся от шлейфа (потребляемый ток должен быть не более 1 мА);

– питающиеся от источника питания 12 В;

– питающиеся от источника питания 24 В;

– питающиеся от сети 220 В 50 Гц.

Контрольные вопросы

1. Какие характеристики электромагнитного поля Вам известны?

2. Как классифицируются контактные преобразователи?

3. Что представляет собой электромагнитный преобразователь?

4. Что представляет собой индуктивный преобразователь?

5. Какие принципы работы преобразователей неэлектрических величин Вам известны? Расскажите о них.

6. Назовите классификацию извещателей.

7. Какие существуют элементы охранно-пожарной сигнализации?

8. Какие существуют наборы для поиска закладных устройств?

9. На что реагируют ионизационные извещатели?

10. В каких извещателях используется эффект Доплера?

Литература

1. Абалмазов Э.И. Направленные микрофоны: мифы и реальность // Специальная техника. – 199. – № 4.

2. Агентство технической безопасности «Нимрод». URL: http://www.nimrod.ru

3. Андрианов, В.И., Соколов А.В. Устройства для защиты объектов и информации: справ. пособие. – 2-е изд. – М.: АСТ; СПб: Полигон, 2000. – 256 с.

4. Баумтрог В.Э. Специальная техника органов внутренних дел: средства общего назначения: учеб.-метод. пособие. – Барнаул: Барнаульский юрид. ин-т МВД России, 2009. – 223 с.

5. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: учеб. пособие. – М.: Горячая линия-Телеком, 2005. – 416 с.

6. Бюро научно-технической информации. URL: http://www.bnti.ru

7. Вандышев Б.А. Использование обратно рассеянного ионизирующего излучения для контроля объектов // Специальная техника. – 1999. – № 3.

8. Власов К.В., Бобров А.Л. Основы вихретокового неразрушающего контроля: учеб. пособие. – Новосибирск: Сиб. гос. ун-т путей сообщения, 2015. – 53 с.

9. Волков В.Г. Наголовные приборы ночного видения // Специальная техника. – 2002. – № 5. – С. 2–15.

10. Гаврилов Л.Н., Демидов В.А., Досычев А.Л. и др. Специальная техника органов внутренних дел: учеб.-нагляд. пособие / под общ. ред. В.П. Сальникова, А.В. Шайтанова. – М.: ИМЦ ГУК МВД России, 2004. – 56 с.

11. Еськов А.В. Средства оперативного визуального наблюдения: учеб. пособие. – Барнаул: Изд-во БЮИ МВД России, 2013. – 33 с.

12. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации: учеб. для вузов / под ред. А.П. Зайцева и А.А. Шелупанова. – М.: Машиностроение, 2009. – 508 с.

13. ЗАО НПЦ Фирма «НЕЛК». URL:www.nelk.ru

14. Ковалев А.В. Поисковые технические средства на основе методов интроскопии. Рентгеновские системы // Специальная техника. – 1999. – № 5. – Ч. 1. – С. 24–27.

15. Ковалев А.В. Поисковые технические средства на основе методов интроскопии. Рентгеновские системы // Специальная техника. – 1999. – № 6. – Ч. 2. – С. 32–38.

16. Ковалев А.В. Поисковые технические средства на основе методов интроскопии. Рентгеновские системы // Специальная техника. –2000. – № 1. – Ч. 3. – С. 22–30.

17. Максимов, Ю.Н., Сонников В.Г., Петров В.Г. и др. Технические методы и средства защиты информации. – СПб.: Полигон, 2000. – 320 с.

18. Петраков, А.В. Основы практической защиты информации: учеб. пособие. – 3-е изд. – М.: Радио и связь, 2001. – 368 с.

19. Савельев И.В. Курс общей физики: учеб. пособие: в 3 т. Т. 2. Электричество и магнетизм. Волны. Оптика. – 7-е изд., стер. – СПб.: Лань, 2007. – 496 с.

1. Сазонов А.А., Лукичев А.Ю., Николаев В.Т. и др. Микроэлектронные устройства автоматики: учеб. пособие для вузов / под ред. А.А. Сазонова. – М.: Энергоатомиздат, 1991. – 384 с.

2. Саликов В.Л. Приборы ночного видения: история поколений // Специальная техника. – 2000. – № 2. – С. 21–32.

3. Современные арочные металлодетекторы. Обзор технологий. URL: http://www.reicom.ru/info/3135 (дата обращения: 02.09.2019).

4. Тюшев А.Н., Лузин А.Н. Курс лекций по физике: учебное пособие для студентов технических специальностей и направлений: в 5 ч. – Новосибирск: Сиб. гос. геод. акад., 2011.

5. Специализированная информационная система «Техника для спецслужб». URL: http://www.sis-tss.ru

6. Специальная техника органов внутренних дел: учеб. / под общ. ред. Ю.А. Агафонова. – Краснодар: Краснод. ун-т МВД России, 2011. – Ч. 1. – 245 с.

7. Сошинов А.Г. Преобразователи неэлектрических величин: учеб. пособие. – Волгоград: ВолгГТУ, 2002. – 36 с.

8. Сюрдо А.И., Бирюков Д.Ю. Физические основы измерений: учеб. пособие. – Екатеринбург: Урал. федер. ун-т, 2013. – 143 с.

9. Хорев А.А. Защита информации от утечки по техническим каналам: учеб. пособие. Ч. 1. Технические каналы утечки информации. – М.: Гостехкомиссия России, 1998. – 320 с.

10. Хорев А.А. Технические каналы утечки акустической (речевой) информации // Специальная техника. – 2009. – № 5. – С. 12–26.

11.Ярочкин В.И. Информационная безопасность: учеб. пособие для студентов вузов. – М.: Международные отношения, 2000. – 400 с.

Оглавление

Учебное издание

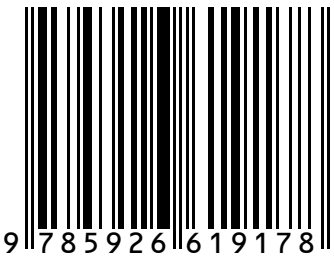
ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Учебное пособие

Составители:
Еськов Александр Васильевич
Победа Александр Сергеевич

Редактор *В. С. Ревина*
Компьютерная верстка *Г. А. Артемовой*

ISBN 978-5-9266-1917-8



Подписано в печать 15.06.2023. Формат 60х84 1/16.
Усл. печ. л. 4,0. Тираж 70 экз. Заказ 153.

Краснодарский университет МВД России.
350005, г. Краснодар, ул. Ярославская, 128.