

Краснодарский университет МВД России

**ФИЗИЧЕСКИЕ ОСНОВЫ ОБРАЗОВАНИЯ
ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ**

Учебное пособие

Краснодар
2023

УДК 004.056.5
ББК 16.84
Ф505

Одобрено
редакционно-издательским советом
Краснодарского университета
МВД России

Рецензенты:

В. Э. Баумтрод, кандидат физико-математических наук, доцент (Барнаулский юридический институт МВД России);

Е. С. Заремба, кандидат юридических наук (Тюменский институт повышения квалификации сотрудников МВД России).

Авторы: *А. В. Еськов, А. С. Победа, М. Ю. Руденко, В. В. Гайфулин*

Физические основы образования технических каналов
Ф505 утечки информации : учебное пособие / А. В. Еськов и др. –
Краснодар : Краснодарский университет МВД России, 2023. – 70 с.

ISBN 978-5-9266-1920-8

Рассматриваются проблемы и технологии, связанные с обнаружением, анализом и предотвращением образования утечек информации через технические каналы. Особое внимание уделяется техническому контролю эффективности мер защиты информации.

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

УДК 004.056.5
ББК 16.84

ISBN 978-5-9266-1920-8

© Краснодарский университет
МВД России, 2023

Введение

Современный этап развития общества в России характеризуется значительным возрастанием осознания важности и вопросов обеспечения безопасности и состояния защищенности информации, находящей свое применение практически всех сферах жизни общества. В частности, в сфере информационной безопасности за последние десятилетия произошло значительное изменение: ответственность за нее перешла из ведения специально предназначенных компетентных служб в могущественную отрасль рыночной производственной экономики.

Очевидно, что несмотря на резкий прогресс, целенаправленное наращивание потенциала и возможностей технической защиты информации, степень безопасности функционирования многосоставных технических систем до сих пор в значительной степени зависит от так называемого «человеческого фактора», суть которого заключается в том числе и в степени профессионализма сотрудника.

В связи с этим, особое значение должно уделяться процессу реализации мер, направленных на качественную планомерную подготовку кадров, а также на своевременное повышение их квалификации – развитие необходимых умений. Данный аспект подразумевает под собой увеличение эффективности наряду с применением в профессиональной деятельности многокомпонентных, составных комплексов.

Знаменательно, что в Указе Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» особая роль отводится вопросу развития и совершенствования системы обучения кадров, в целях формирования у них надлежащих компетенций. В допол-

нение к Указу Президента, российское законодательство постоянно обновляется в целях формирования устойчивости к новым угрозам в сфере информационной безопасности. Это подразумевает непрерывный процесс разработки и реализации новых законов и нормативных актов, направленных на защиту государственной или частной информации.

Также для реализации решений, выдвинутых со стороны государственного управления, особенно остро ставится вопрос об улучшении качества подготовки и обучения кадрового состава. Данная необходимость обусловлена значительным недостатком квалифицированных кадров в области безопасности современных информационных технологий. В этих целях Российская Федерация активно участвует в международных инициативах по безопасности информационных технологий, сотрудничая с другими странами и международными организациями в обмене знаниями и опытом в этой области. Это сотрудничество чрезвычайно значимо для повышения глобальной устойчивости к угрозам. На уровне государства изучение этой темы критически важно для поддержания правопорядка, предотвращения шпионажа и защиты национальной безопасности. Правительства и спецслужбы используют знания в этой области для разработки стратегий национальной безопасности и противодействия внешним и внутренним угрозам.

Изучение данной темы также способствует проведению научных исследований и развитию инноваций в области информационной безопасности. Понимание физических процессов, лежащих в основе образования технических каналов утечки информации, открывает пути для новаторских решений и улучшения существующих методов защиты, а также необходимо для проведения аудитов безопасности и оценки рисков в ор-

ганизациях. Это позволяет выявлять потенциальные уязвимости и разрабатывать стратегии управления рисками, а также обеспечивает соответствие нормативным требованиям в области безопасности. В целом, значимость этой темы неуклонно растет в условиях, когда обеспечение конфиденциальности и целостности информации становится все более критическим для государственных структур и ведомств.

В данном учебном пособии авторы, используя системный подход, представили вопросы и рассмотрели проблемы и технологии, связанные с обнаружением, анализом и предотвращением образования утечек информации через технические каналы, уделяя особое внимание методам и средствам, применяемым в области технической защиты информации и касающимся управления и реализации задач по защите от утечки информации через технические каналы с использованием существующей литературы, опираясь на профессиональный и научный опыт. Это направление объединяет знания физики, информатики и техники безопасности, предоставляя разъяснения механизмов, через которые конфиденциальная информация может быть невольно раскрыта или украдена.

1. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ПРОВОДНЫХ КАНАЛОВ ПЕРЕДАЧИ ИНФОРМАЦИИ

1.1. Понятие и классификация технических каналов утечки информации

Когда мы говорим о формировании потенциальных каналов утечки информации, особенно важными являются основные технические средства приёма, 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 распределёнными параметрами образуют распределённые случайные антенны: интерфейсы, трубы.

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

Наиболее распространенным каналом утечки информации – электромагнитный, образующийся из-за различного рода 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 перехватываться средствами контроля, например, каналы конвенциональной радиосвязи, Wi-Fi, Bluetooth.

Наиболее доступной информацией, передаваемой путем ПЭМИН, – это данные, вводимые с клавиатуры компьютера или отображаемые на мониторе и передаваемой по соединительному кабелю к системному блоку ПК.

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.

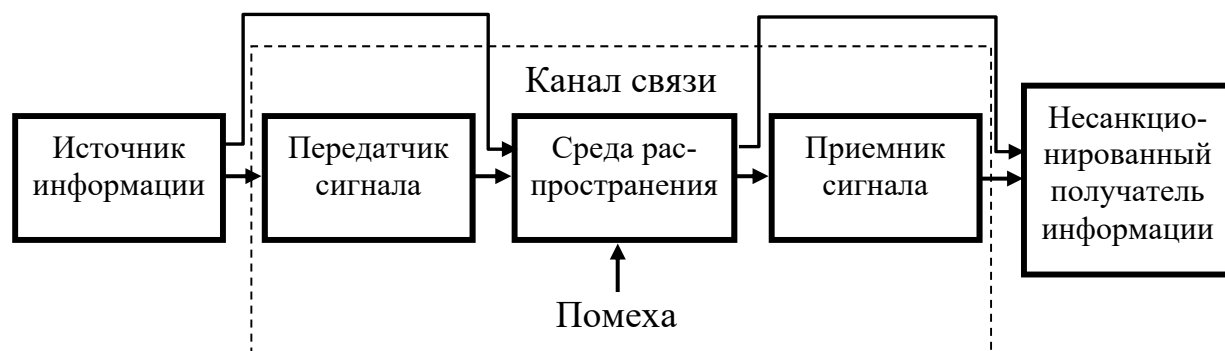


Рис. 1. Структура технического канала утечки информации

Информация от источника поступает на вход канала в формате источника, передатчик преобразует поступающую информацию в формат, соответствующий ее записи на носитель 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.

Съём информации, передаваемой по проводным линиям связи, реализуется с помощью электронных устройств, подключаемых к линиям параллельно (одновременно к двум проводам) (рис. 2, а), последовательно (в разрыв одного из проводов) (рис. 2, б) и с использованием индукционного датчика (бесконтактное подключение, рис. 3).

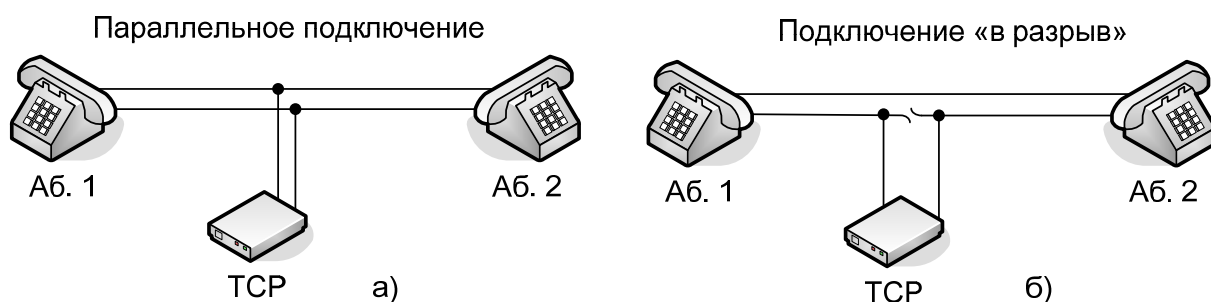


Рис. 2. Подключение закладного устройства к линии связи

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 $\frac{U}{R_{\Sigma}} = \frac{U}{R_1} + \frac{U}{R_2}$, где R_{Σ} – эквивалентное сопротивление всех параллельно соединенных сопротивлений.

Сократив на общий множитель U , имеем $\frac{1}{R_{\Sigma}} = \frac{1}{R_1} + \frac{1}{R_2}$. В последнем выражении приведем правую часть к общему знаменателю $\frac{1}{R_{\Sigma}} = \frac{R_1 + R_2}{R_1 \cdot R_2}$. Определим R_{Σ} $R_{\Sigma} = \frac{R_1 \cdot R_2}{R_1 + R_2}$.

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

Учитывая, что при параллельном соединении напряжение на элементах одинаково, можно записать $i_1 R_1 = i_2 R_2 = i R_{\Sigma}$. 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 $U_K = iU_K$.

Подставляя в исходную формулу вместо напряжений соответствующие им выражения, получаем $iR_{\Sigma} = iR_1 + iR_2$, где R_{Σ} — эквивалентное (общее) сопротивление всех последовательно соединенных сопротивлений. Сократив на общий множитель i , имеем $R_{\Sigma} = R_1 + R_2$.

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, или 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.

Как только рядом с телефонной линией устанавливается индуктивный датчик (см. рис. 3), он начнет генерировать ЭДС, значение которой зависит от мощности сигнала, передаваемого по этой линии.

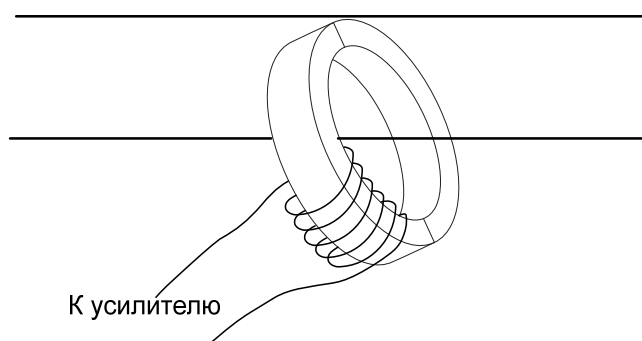


Рис. 3. Подключение к линии индуктивного датчика.

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), емкость 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 и, как правило, они имеют меньшие размеры.

Следует заметить, 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.

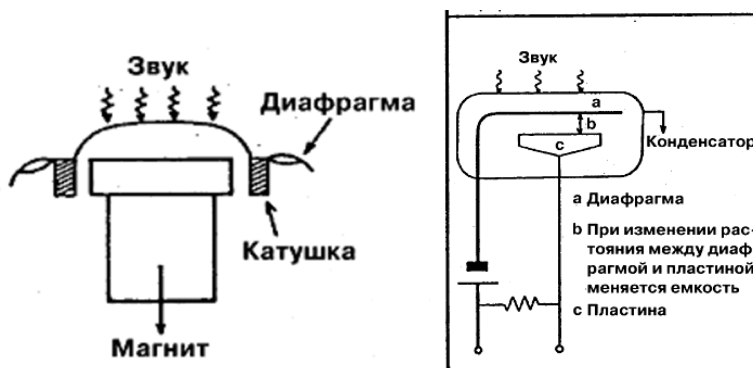


Рис. 4. Устройство электродинамического (слева) и конденсаторного (справа) микрофонов

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, то 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 служат для акустического контроля источников звуков в открытой местности.

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

Устройства технического контроля проводных линий применяются для выявления потенциально опасных сигналов и их источников, включая скрытые устройства. Основными маршрутами для передачи электрических сигналов, содержащих информацию от таких устройств, являются телефонные линии и электропитающие цепи. Так, в состав средств контроля проводных линий связи и подавления проводных подслушивающих устройств входят устройства и приборы для контроля телефонных линий и линий электропитания.

Для контроля телефонных линий используются методы, которые базируются на изменениях электрических характеристик линий, вызываемых подключениями к ним.

Например, вариация следующих характеристик:
напряжения в линии;

тока в линии;
значений емкости;
значений индуктивности;
значений активного и реактивного сопротивлений.

В зависимости от способа подключения подслушивающего устройства к телефонной линии (последовательное подключение в разрыв провода телефонного кабеля, параллельное или индуктивное), воздействие такого устройства может значительно различаться. Поскольку закладные устройства являются активными, величина мощности, извлекаемой из телефонной линии, зависит от мощности передатчика закладки и его входного сопротивления. Изменения этих параметров могут обнаружить наличие подслушивающего устройства при опущенной трубке телефонного аппарата. Что касается контроля линий электропитания, он осуществляется путем измерения электрических параметров линий, таких как напряжение, ток, активное и реактивное сопротивление.

Это позволяет обнаруживать закладные устройства, которые могут быть подключены к линиям электропитания. Помимо телефонных линий и линий электропитания, существуют также 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 отрас-

лях, включая правоохранительные органы, корпоративный сектор и государственные учреждения.

Простейшее устройство контроля телефонных линий представляет собой измеритель напряжения с индикацией конфигурации его значения от обычного, которое фиксируется оператором, работая в режиме настройки вращением 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.

Поскольку любое физическое подключение к кабелю телефонной линии создает в ней неоднородность, от которой отражается посылаемый 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).

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 наличии последовательного или параллельного гальванического соединения устройств для сбора информации их

питание осуществляется от телефонной линии. В то же время существуют устройства с компенсацией падения напряжения в телефонной линии, а при использовании бесконтактного подхода устройства работают от автономного источника питания. Полученная информация, как правило, передается по радиоканалу.

Радиопередающее устройство активируется только во время телефонного разговора. Кроме того, такие устройства могут выполнять функцию записи речевой информации на магнитный носитель или использовать другой физический принцип хранения информации. Устройство записи активируется только при ведении разговора. Возможно также прослушивание разговоров путем подключения другого телефонного аппарата в смежной комнате.

Рассмотрим методы подавления проводных подслушивающих устройств:

1. Подача в телефонную линию синфазного маскирующего низкочастотного сигнала во время разговора (метод синфазной низкочастотной маскирующей помехи).

2. Подача в телефонную линию маскирующего высокочастотного сигнала звукового диапазона во время разговора (метод высокочастотной маскирующей помехи).

3. Подача в телефонную линию маскирующего ультразвукового сигнала во время разговора (метод ультразвуковой маскирующей помехи).

4. Поднятие напряжения в телефонной линии во время разговора (метод повышения напряжения).

5. Подача маскирующего сигнала, компенсирующего постоянную составляющую телефонного сигнала во время разговора (метод «обнуления»).

6. Подача маскирующего низкочастотного сигнала в линию при положенной телефонной трубке во время разговора (метод низкочастотной маскирующей помехи).

7. Подача маскирующего низкочастотного сигнала при приеме сообщений с известным спектром в линию (компенсационный метод).

8. Подача высоковольтных импульсов в телефонную линию (метод «выжигания»).

Смысл метода синфазной низкочастотной маскирующей помехи состоит в передаче идентичных помеховых сигналов речевого спектра частот в оба провода телефонной линии с помощью общей системы заземления АТС и нулевого провода электрической сети 220 В (причем нулевой провод электрической сети заземлен). Эти помеховые сигналы имеют согласованные амплитуды и фазы, обычно наибольшая мощность помехи сосредоточена в диапазоне частот стандартного телефонного канала: 300 ... 3400 Гц. В телефонном аппарате эти помеховые сигналы взаимно уничтожаются, что предотвращает их влияние на передачу полезного сигнала (разговор по телефону). Однако при снятии информации с одного провода телефонной линии помеховый сигнал не может быть устранен. Ввиду того, что его уровень значительно превышает уровень полезного сигнала, перехват информации (извлечение полезного сигнала) становится технически осуществимым.

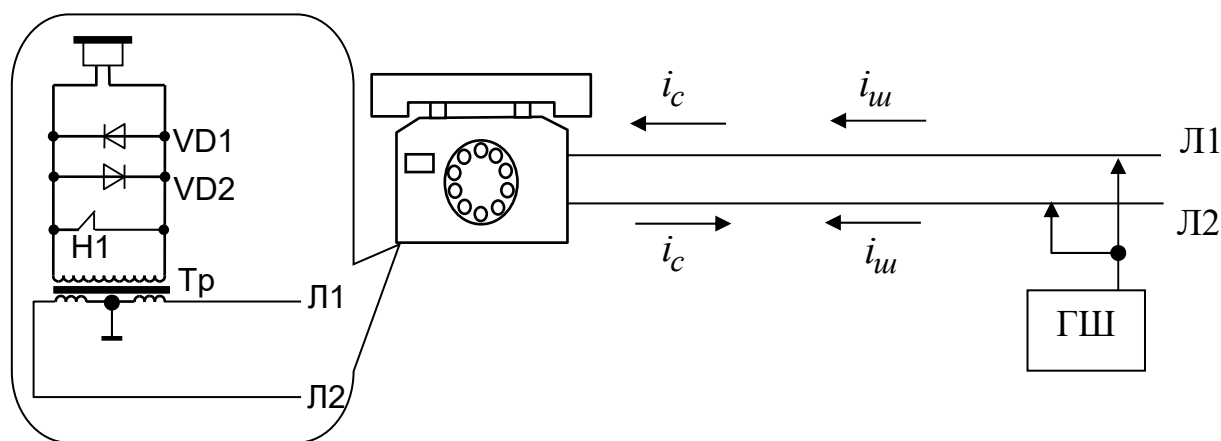


Рис. 5. Принцип метода синфазного маскирующего сигнала

Так, цифровые сигналы речевого спектра частот, представленные последовательностью импульсов, образованных псевдослучайным способом, применяются в качестве маскирующего помехового сигнала.

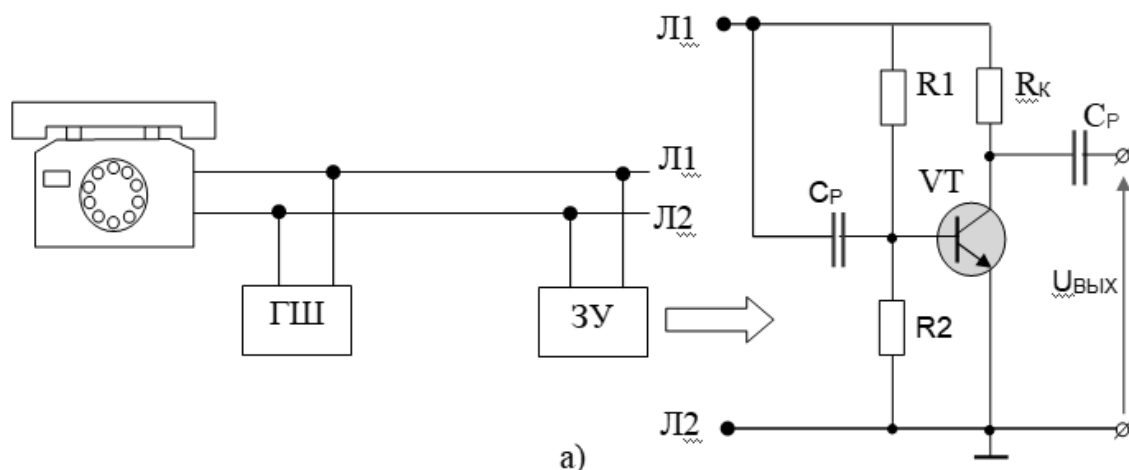
Способ синфазного маскирующего низкочастотного сигнала используется для намеренной поломки телефонных закладок (как с параметрической, так и с кварцевой стабилизацией частоты) с последовательным (в разрыв одного из проводов) включением, а также телефонных радиозакладок и диктофонов с подключением к линии (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 (то есть 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 (осо-

бенно, не имеющих предусилителей) существенно ниже, чем средств с гальваническим подключением к телефонной полосе.

В качестве маскирующего сигнала используются широкополосные аналоговые сигналы, наподобие «белого шума», или цифровые сигналы, представляющие собой псевдослучайные последовательности импульсов. Частоты маскирующих сигналов подбираются таким образом, чтобы их уровень был достаточным для подавления полезного сигнала, но в то же время не ухудшалось качество телефонных разговоров. Чем ниже частота помехи, тем сильнее её воздействие и большая помеховая мощность на нужный сигнал. В основном используются частоты в диапазоне от 6 до 8 кГц до 16 до 20 кГц. Для уменьшения вероятности воздействия помехового маскирующего сигнала на телефонный разговор в устройстве защиты активируется специальный низкочастотный фильтр с граничной частотой 3,4 кГц, который подавляет помеховые сигналы, не сильно влияя на передачу полезных сигналов.

Способ ультразвуковой маскирующей помехи в основном аналогичен описанному выше. Отличие заключается в том, что здесь используются помеховые сигналы ультразвукового диапазона с частотами от 20 до 25 кГц до 50 до 100 кГц.



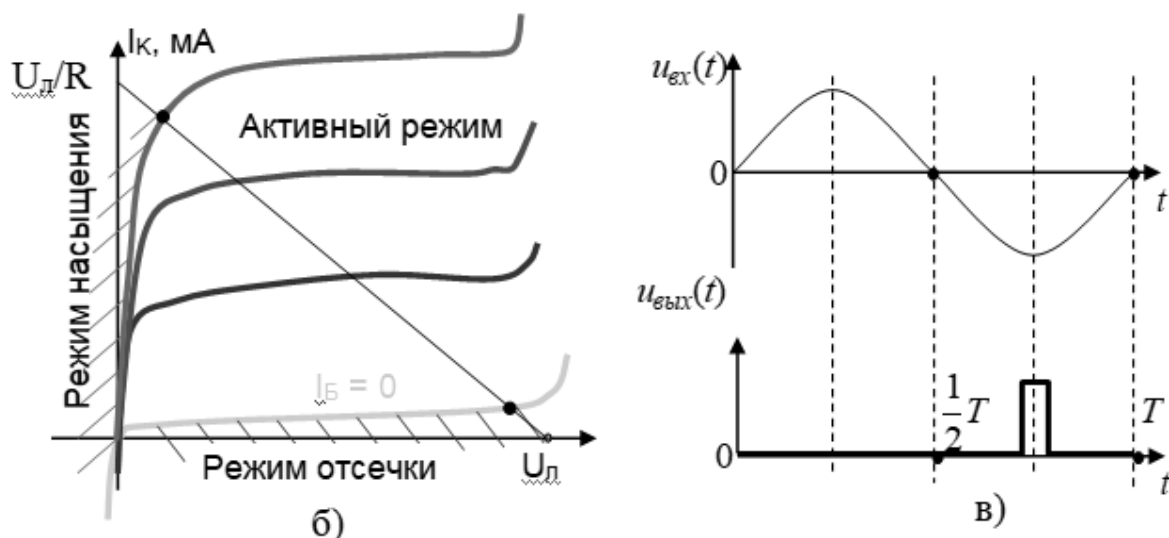


Рис. 6. Принцип ультразвукового подавления

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 влечёт у радиозакладок с последовательным подключением и параметрической стабилизацией частоты «уход» несущей частоты и уменьшения 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 напряжению 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 и 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 под собой подачу в линию при положенной трубке стационарного телефонного аппарата маскирующего сигнала (наиболее часто, типа «белого шума») речевого спектра частот (важно, чтобы основная мощность помехи заключалась в спектре частот обычного телефонного канала: 300 ... 3400 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.

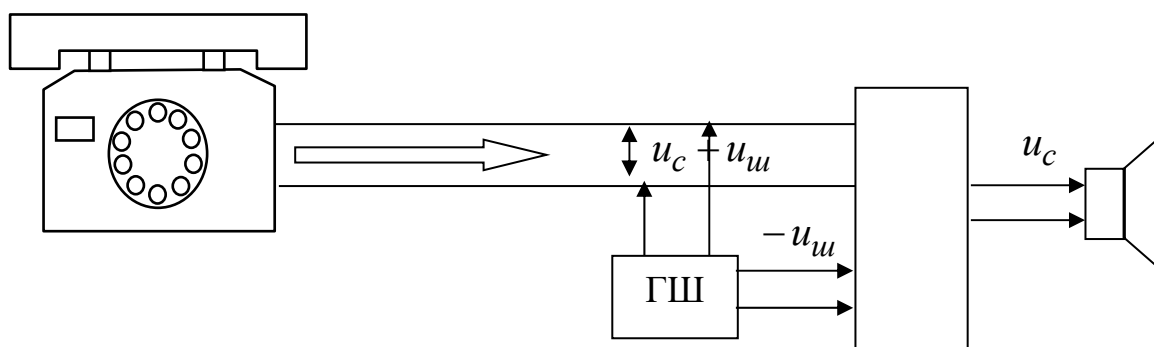


Рис. 7. Принцип компенсационного метода подавления

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 адаптивного 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 1500 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 ли-

нию производится два раза. Первый (для «выжигания» параллельно подключенных устройств) – при разомкнутой телефонной линии, второй (для «выжигания» последовательно подключенных устройств) – при замкнутой (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, которое не имеет отношения к перехвату информации и подключенное к телефонной линии. 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/Т», «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/Т», «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 1500 ... 1600 В. Мощность «выжигающих» импульсов составляет 15 ... 50 ВА. 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 секунд до 24 часов.

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

Вместе со средствами активной защиты в практическом применении часто применяются 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 130 ... 160 Ом для каждой пары, а для проводов марки ТРП и ТРВ имеет разброс 220 ... 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.

Также существуют 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 ли-

нии (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 минуты 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 секунд) 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 препятствования работе (набору номера) незаконно подключенных параллельных телефонных устройств используют специальные электронные блокираторы. Объясним принцип их функционирования на примере устройства под названием «Рубин». В обычном режиме устройство анализирует состояние телефонной линии путем сравнения напряжения в линии с эталонным напряжением на специальной нагрузке, подключенной к цепи телефонного аппарата. Когда незаконно подключенный параллельный телефонный аппарат поднимает трубку, напряжение в линии снижается, что фиксируется устройством защиты. Если это происходит во время телефонного разговора, срабатывает звуковая и световая сигнализация (нарушение подключения к линии подтверждается загоранием светодиода). А если факт незаконного подключения обнаружен

в момент, когда не ведется разговор (трубка на защищенном телефонном аппарате не поднята), то срабатывает сигнализация, и устройство защиты переходит в режим блокирования набора номера с параллельного телефонного аппарата. В этом режиме устройство защиты создает обходную цепь для телефонной линии с сопротивлением 600 Ом (имитируется положение трубки на защищенном телефонном аппарате), что полностью исключает возможность набора номера с параллельного телефонного аппарата. Кроме обнаружения незаконного подключения к линии параллельного телефонного аппарата, устройство защиты «Рубин» также сигнализирует о разрыве (отключении) и коротком замыкании телефонной линии.

1.5. 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. ОБРАЗОВАНИЕ И ЗАЩИТА ОТ 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.

Методы защиты с помощью инженерных конструкций в совокупности с техническими средствами охраны формируют физическую защиту.

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 другие.

Классификация методов защиты представлена на рис. 8.

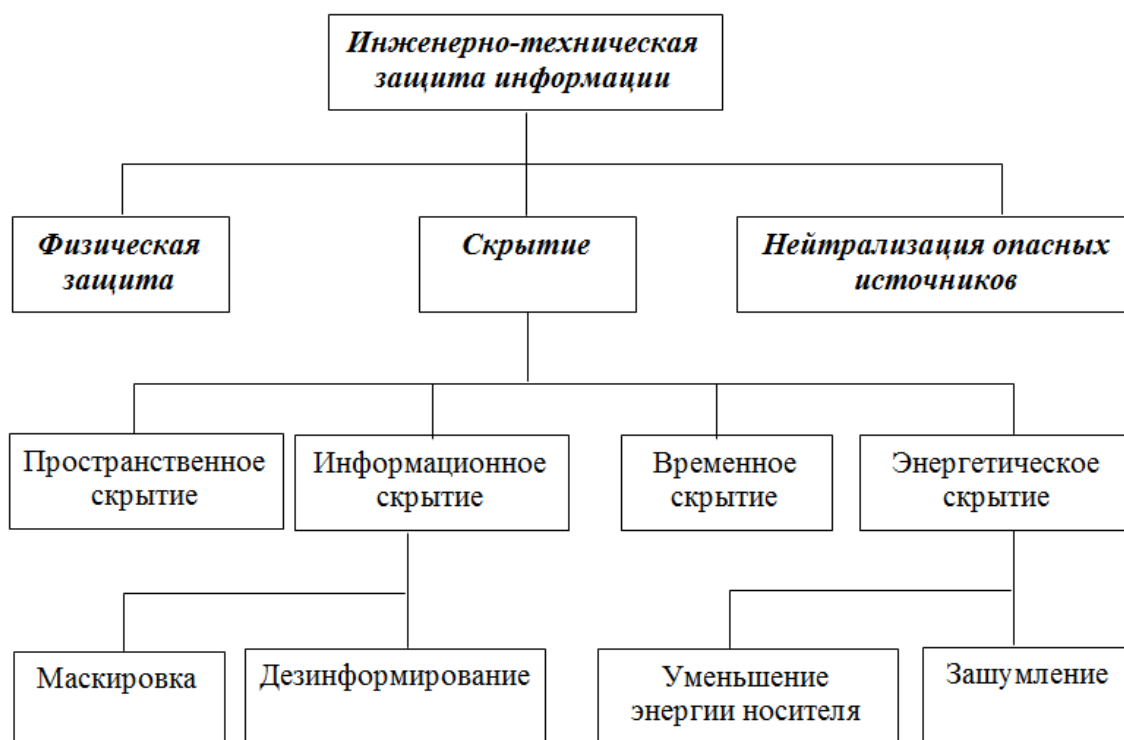


Рис. 8. Классификация направлений и методов ИТЗИ

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

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 изменяться 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 определяет дальность распространения информационного сигнала в диапазоне радиоволн.

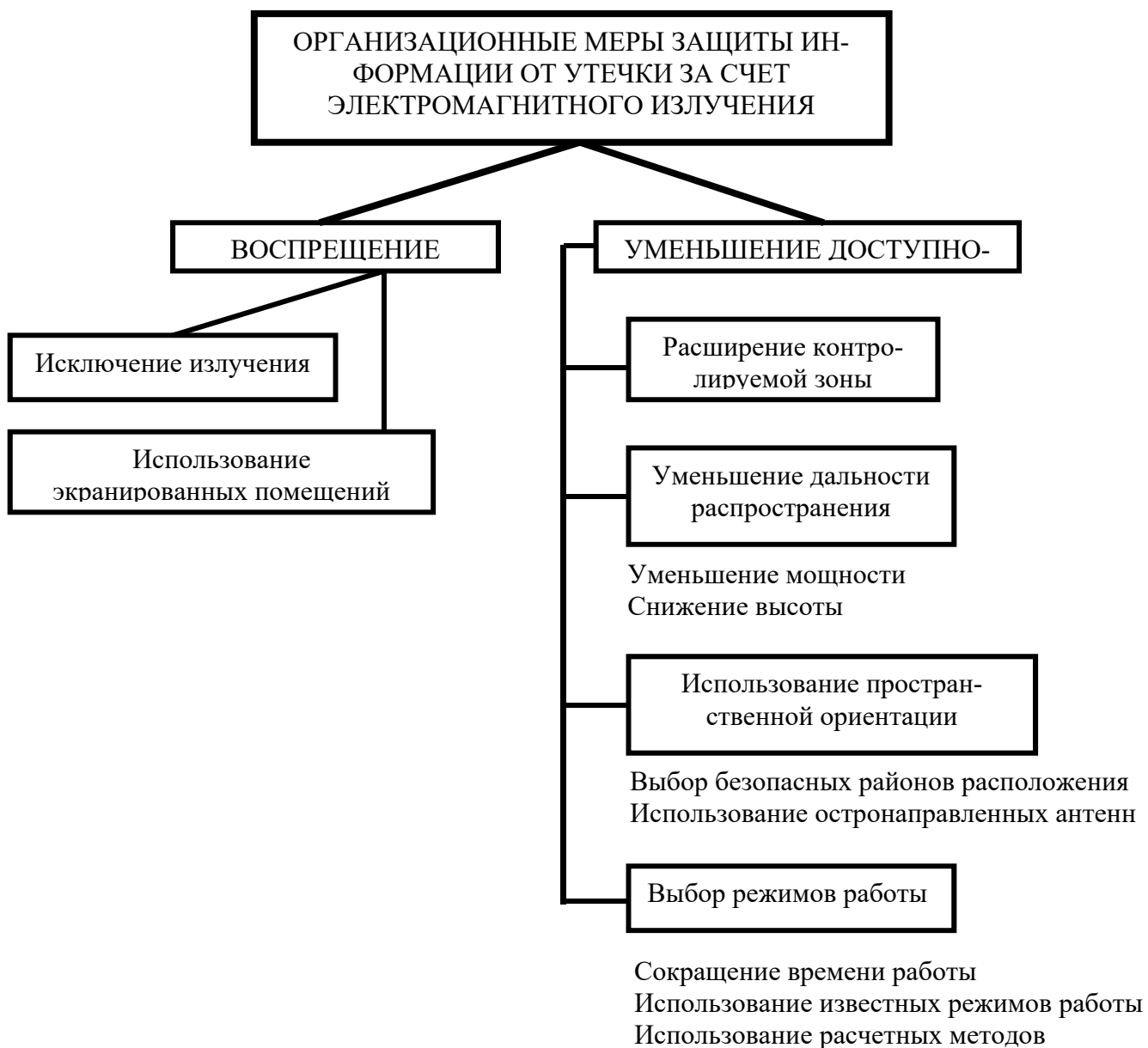


Рис. 9. Организационные меры защиты от утечки информации за счет ПЭМИН

2.2. Пассивные методы защиты от утечки за счет ПЭМИН

Электронные устройства, работающие при высоком напряжении и низком токе, порождают электромагнитные поля, в которых электрическая составляющая преобладает в непосредственной близости. Если компоненты электроники нечувствительны к магнитной составляющей, электрические поля оказывают на них наибольшее воздействие.

В свою очередь, устройства электроники, работающие при больших токах и малых изменениях напряжения, порождают электромагнитные поля, в которых преобладает магнитная составляющая в ближней зоне. Если компоненты электроники нечувствительны к электрической составляющей, магнитные поля оказывают на них наибольшее воздействие. Также, соединительные линии, такие как провода и кабели создают 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 ключевой 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 ис-

пользовать 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 способом снижения уровня побочных электромагнитных излучений является применение экранирования для их источников.

Существуют несколько методов экранирования:

- электростатическое;
- магнитостатическое;
- электромагнитное.

Электростатическое и магнитостатическое экранирование основано на облицовке экраном (в первом случае с высокой электропроводностью, а во втором – с магнитной проводимостью) соответственно электрических и магнитных полей.

Основной целью экранирования электрических полей является уменьшение емкости связи между экранируемыми частями конструкции. Следовательно, положительные результаты экранирования в основном проявляются в сокращении емкостной связи между источником и приемником помех до и после установки заземленного экрана. Поэтому любые усилия, направленные на снижение этой емкости связи, повышают эффективность экранирования.

2.3. Активные меры защиты информации от утечки за счет ПЭМИН

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:

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

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.

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 5-10 раз.

Средства активной защиты подразделяются 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 (СЛЗ) применяются при необходимости снижения электромагнитных помех и защиты от перехвата информации при случаях:

недостаточных уровней переходных затуханий между влияющими и подверженными влиянию кабелями и соединительными линиями;

воздействия на цепи, провода и устройства вспомогательной аппаратуры низкочастотных электромагнитных полей основной аппаратуры;

наличия электроакустических преобразований во вспомогательной аппаратуре.

Примеры использования:

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 подавления используются, когда невозможно обеспечить необходимое разделение проводов, вы-

ходящих за пределы контролируемой зоны и технических средств обработки информации (то есть не выполняется требование по Зоне № 1), но при этом удовлетворяется требование по Зоне № 2 (то есть расстояние от технических средств обработки информации до границы контролируемой зоны больше, чем Зона № 2).

В этом случае генератор шума может подключаться к линии по симметричной и несимметричной схемам (рис. 10).

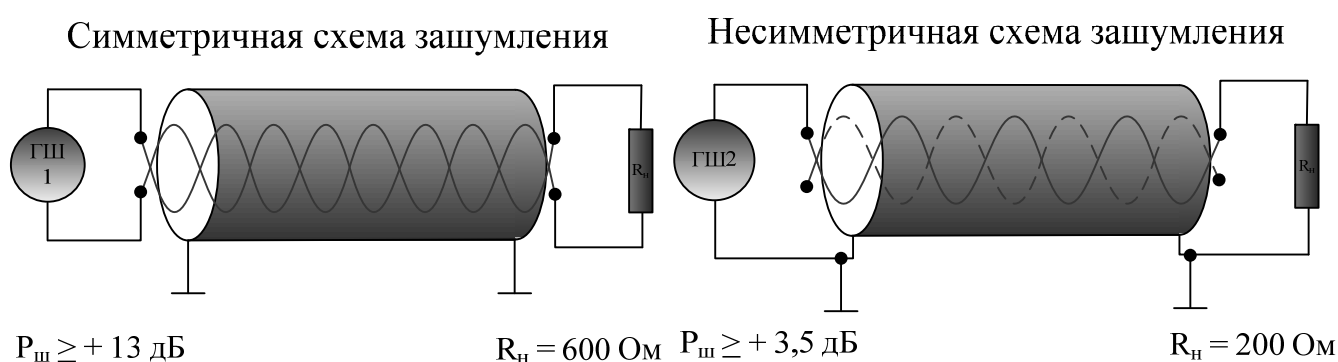


Рис. 10. Несимметричная и симметричная схемы зашумления

По несимметричной схеме генератор шума подключается в центральный повив кабеля (ГШ1 на рис. 11), по несимметричной – во внешний (ГШ2, ГШ3 на рис. 11).

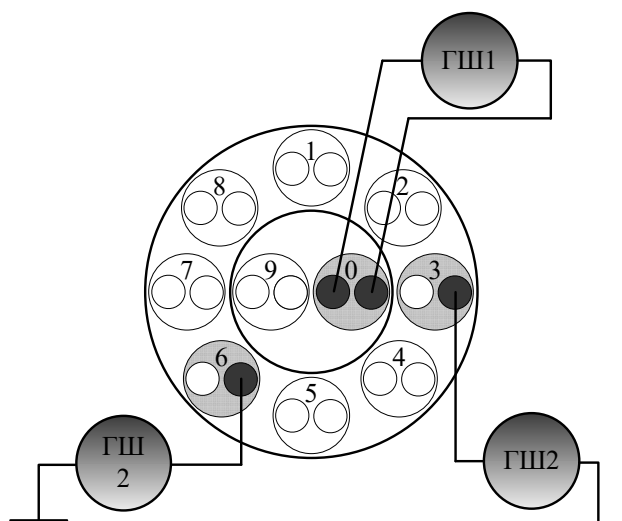


Рис. 11. Вариант подключения генератора шума

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 устанавливается так, чтобы «кабельные петли» находились в трех ортогональных плоскостях. В зависимости от конкретных условий каждая «кабельная петля» может быть создана с использованием одного или нескольких целых витков, при этом витки могут быть сконцентрированы в одной плоскости (сформированные отдельными жилами одного кабеля) или в параллельных плоскостях. Выбор количества витков для системы пространственного электромагнитного зашумления коллективной (СПЗ-К) определяется раз-

мерами 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 зашумления в основном используются помехи типа «белого шума» 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, При вводе в эксплуатацию системы пространственного зашумления необходимо проводить специальные исследования по требованиям обеспечения электромагнитной совместимости (ЭМС).

2.6. 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 восприятие?

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 $T=2\pi/\omega$.

Число колебаний в единицу времени есть частота $f=1/T$. Единица измерения частоты в СИ – герц (Гц), $1 \text{ Гц} = 1 \text{ с}^{-1}$, $\omega=2\pi/T=2\pi f$.

Круговая частота ω (циклическая) в 2π раз больше частоты колебаний f и 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. Это ситуация называется резонансом, а частота $\omega_{\text{рез}}$ – резонансной частотой $\omega_{\text{рез}} = \sqrt{\omega_0^2 - 2\delta^2}$. При $\omega_0^2 < 2\delta^2$ резонанс отсутствует.

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

Отсюда, при уменьшении коэффициента затухания δ резонансная амплитуда возрастет ($\delta \rightarrow 0$, $A_{рез} \rightarrow \infty$), 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 $U(t)$:

$$U(t) = M[X(t), B(t)].$$

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

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

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_m и начальной фазой, равной нулю:

$$u_m(t) = U_m \cos \Omega t .$$

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

$$u_n(t) = U_n \cos(\omega_0 t + \psi) .$$

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

$$U_n(t) = U_n + a_{AM} U_m \cos \Omega t ,$$

где a_{AM} — коэффициент пропорциональности.

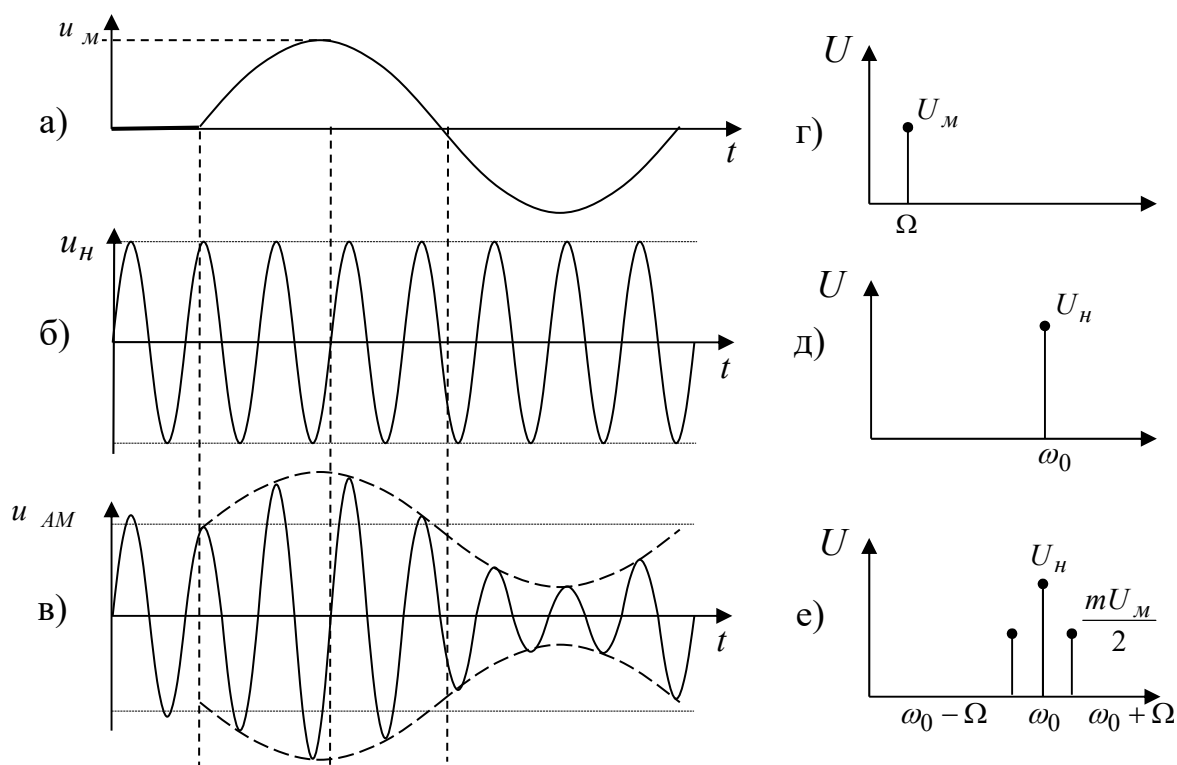


Рис. 12. Сигналы и их спектры при АМ гармонического колебания

Подставляя в последнее выражение вместо U_H из предпоследнего, получим

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

описывающее АМ сигнал на любом интервале времени.

На рис. 12, а-в приведены соответствующие графики функций. Огибающая изображена на этом рисунке штриховой линией.

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

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

Таким образом, спектр АМ-сигнала можно рассматривать как сумму трех гармонических колебаний: $u_n(t)$ с амплитудой U_n и частотой ω_0 , с амплитудой $mU_n/2$ и частотой $\omega_0 - \Omega$ и, наконец, с амплитудой $mU_n/2$ 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 $m_q \ll 1$ аналогичен спектру АМ-сигнала и также состоит из несущего колебания и двух боковых составляющих с частотами $\omega_0 + \Omega$ и $\omega_0 - \Omega$.

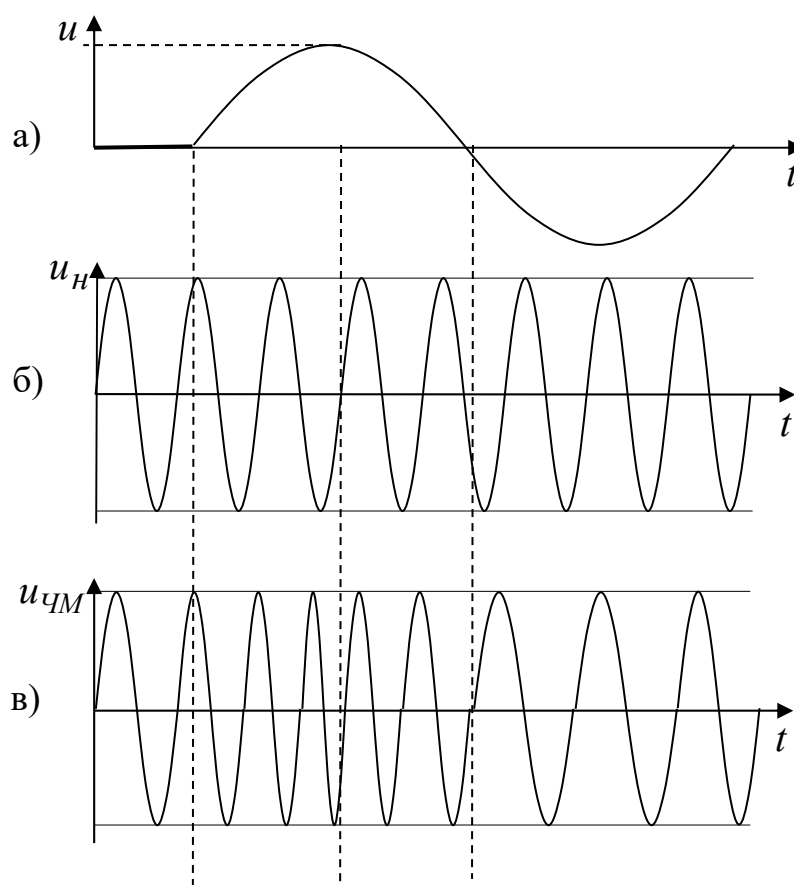


Рис. 13. Частотно модулированный сигнал

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

$$\Delta \omega_{y.m} = 2(m + 1)\Omega.$$

ЧМ- и ФМ-сигналы, применяемые на практике, имеют индекс модуляции $m_{\omega} \gg 1$, поэтому:

$$\Delta\omega_{\omega\mu} = 2m\Omega.$$

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

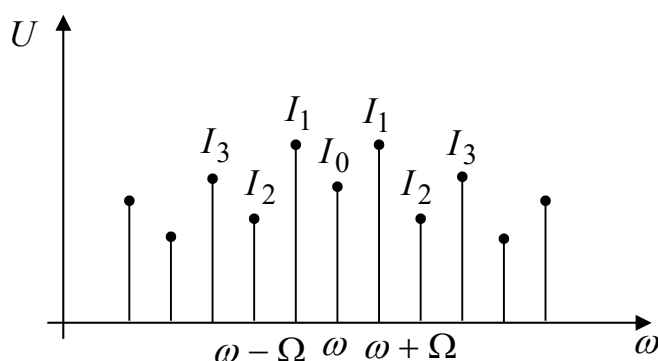


Рис. 14. Спектр частотно-модулированного сигнала

К узкополосной модуляции относятся все виды модуляции АМ, 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.

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. С другой стороны, 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 необходимо не столько энергетические, сколько информационные составляющие процесса. Наиболее перспективным направлением прогрессирования измерительной техники относительно к задаче анализа информативности побочных излучений и наводок в низкочастотном диапазоне

следует отметить появление измерительных регистраторов электрических величин на базе скоростных АЦП.

На рынке наиболее передовые приборы общего назначения такого типа выпускает компания Hewlett 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 одиночной записи и достигает единиц микровольт в режиме накопления. Регистраторы совместимы со стандартным интерфейсом для персональных компьютеров, что позволяет в процессе обработки результатов измерений гибко создавать систему параметров, наиболее точно описывающую измеряемые данные.

В наше время наблюдается тенденция создания измерительно-вычислительных комплексов на основе ПЭВМ, использующих адаптеры для ввода аналоговых сигналов. Общий результат выходит сходный, однако в первом случае развитие происходит через усовершенствование измерительного прибора, в то время как во втором – через ПЭВМ. На данный момент комплексы, основанные на измерительных приборах, обладают большей чувствительностью и широким частотным диапазоном, в то время как комплексы, основанные на ПЭВМ, отличаются многоканальностью и развитыми пакетами обработки и визуализации сигналов.

Способы и средства обнаружения каналов утечки информации включают в себя:

1. Проверка сетевых настроек: это может включать проверку конфигурации брандмауэра, настройки доступа к сети, обнаружение несанкционированных точек доступа Wi-Fi.

2. Мониторинг событий безопасности: это может включать мониторинг аномальной активности или изменений в сети, обнаружение несанкционированных доступов, мониторинг использования несанкционированных устройств.

3. Использование специализированного программного обеспечения: это может включать использование программных средств для обнаружения сетевых уязвимостей, к которым могут обращаться злоумышленники, обнаружение утечки данных, мониторинг наличия шпионского или вредоносного ПО.

4. Физический обход: это 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: это 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 показывают эффективный результат, если имеется в конфигурации специальное, синхронизированное с АЦП формирование информативных сигналов в исследуемом объекте. Используемые в современном мире франшизы генераторов синусоидальных и импульсных сигналов в этом случае недостаточны. Имеющиеся на данном этапе логические анализаторы и формирователи тестовых сигналов обычно создаются для выполнения других задач функционального контроля аппаратуры. Ввиду чего проблема использования стимулирующего воздействия на рассматривае-

мый 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. подсчеты.

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

Таким образом, проанализировав настоящее состояние аппаратной базы и прогресса ее развития, базовым для осуществления измерений при оценке каналов утечки необходимо принять на текущий момент – 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 параграфе,

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 комплекты средств для уборки помещений. Рациональным выбором будет покупка средств, которые окупятся в течение 5 лет по сравнению с расходами на уборку помещений при использовании арендованных средств или услуг специализированных компаний. Обычно набор средств для обнаружения подслушивающих устройств можно разделить на три категории: минимальные, средние и максимальные.

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.).

Таким образом, разумно объединить ее со сканирующим приемником и использовать программное обеспечение Sedif или FIJLIN для автоматизированного анализа радиообстановки в помещении. Так появится высшая вероятность обнаружения радиозакладных устройств. Цена подобного набора (без компьютера) – 50000-75000 руб., но он не осуществляет надлежащего качества выявления закладных устройств, закладок дистанционно-управляемых, подключенных к электросети или размещаемых в железобетонных стенах.

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 нежелательных электромагнитных излучений и помех нужно определить параметры интенсивности поля в окружающем пространстве или токов и напряжений в цепях, возникающих в результате электрических процессов для создания информационных сигналов. Использование данных параметров позволяет более эффективно выявлять скрытые устройства, чем радиомониторинг 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 служат для определения стандартных параметров электромагнитных процессов. Однако, множество измерительных приборов ориентировано 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 ВУ, оснащенные радиоуправляемыми детонаторами и/или взрывателями с электронными таймерами. Традиционным средством поиска таких ВУ 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 способности обнаруживать радиоэлектронные устройства с нелинейными вольтамперными характеристиками, такими 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 нелинейно-

го 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.

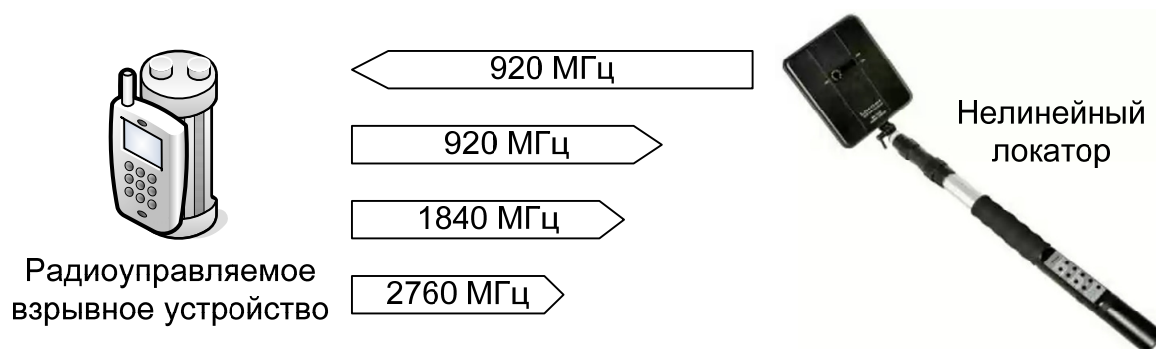


Рис. 15. Принцип нелинейной локации

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 и 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.

Прибор приемно-контрольный – 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 укреплённости 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



Рис. 16. Классификация извещателей

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.

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 их 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 не отапливаемых 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.

3.5. 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?

Заключение

Учебное пособие «Техническая защита информации» подготовлено для изучения одноименной дисциплины с учетом ранее изученных материалов по дисциплине «Физика». Предназначено для подготовки курсантов, обучаемых по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере к освоению дисциплин, изучаемых на кафедре информационной безопасности Краснодарского университета МВД России: «Техническая защита информации», «Системы связи», «Специальная техника органов внутренних дел». Знания о физических основах утечки информации способствует разработке более продвинутых и надежных технологий защиты. Это включает в себя создание защищенного оборудования, программного обеспечения и коммуникационных протоколов.

В пособии приводится описание и принцип работы технических средств защиты информации, описание технических каналов связи, описание и принцип работы средств поиска устройств съема информации с технических каналов связи. Это обеспечивает осведомленность и компетенции сотрудников, повышая общий уровень безопасности как государственных, так и коммерческих организаций. Сотрудники, обладающие знаниями в этой области, могут лучше распознавать потенциальные угрозы и эффективно предотвращать утечки данных.

Учебное пособие может быть использовано курсантами и слушателями при дополнительной подготовке к занятиям по дисциплине «Специальная техника ОВД» различных специальностей.

Литература

1. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009. – 508 с.

2. Андрианов, В.И., Соколов А.В. Устройства для защиты объектов и информации: Справочное пособие. – 2-е изд. – М.: ООО «Фирма «Издательство АСТ»; СПб: ООО «Издательство «Полигон», 2000. – 256 с.

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

4. Максимов, Ю.Н., Сонников В.Г., Петров В.Г. и др. Технические методы и средства защиты информации. – СПб.: ООО «Издательство Полигон», 2000. – 320 с.

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

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

7. ЗАО НПЦ Фирма «НЕЛК» www.nelk.ru

8. Гаврилов Л.Н., Демидов В.А., Досычев А.Л. и др. Специальная техника органов внутренних дел: учебно-наглядное пособие/ под общей редакцией В.П. Сальникова, А.В. Шайтанова. – М.: ИМЦ ГУК МВД России, 2004. – 56 с.

9. Баумтрог В.Э. Специальная техника органов внутренних дел: средства общего назначения: Учебно-методическое пособие. – Барнаул: Барнаульский юридический институт МВД России, 2009. – 223 с.

10. Савельев И.В. Курс общей физики: в 3-х т. Т. 2. Электричество и магнетизм. Волны. Оптика: учебное пособие. – 7-е изд., стер. – СПб.: Изд-во «Лань», 2007. – 496 с.

11. Курс лекций по физике: учебное пособие для студентов технических специальностей и направлений: [в 5 ч.] / А. Н. Тюшев, А. Н. Лузин; М-во образования и науки Российской Федерации, ГОУ ВПО «Сибирская гос. геодезическая акад.» Новосибирск : СГГА, 2011.

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

13. Ковалев А. В. Поисковые технические средства на основе методов интроскопии. Рентгеновские системы// Специальная техника – 1999. –№5-6; 2000. – № 1.

14. Современные арочные металлодетекторы. Обзор технологий. Режим доступа: <http://www.reicom.ru/info/3135> (02.09.2019).

15. Микроэлектронные устройства автоматики: Учеб. пособие для вузов / А.А. Сазонов, А.Ю. Лукичев, В.Т. Николаев и др.; Под ред. А.А. Сазонова. – М.: Энергоатомиздат, 1991. – 384 с.

16. Хорев А.А. Защита информации от утечки по техническим каналам. Часть1. Технические каналы утечки информации. Учебное пособие. М.: Гостехкомиссия России, 1998. – 320 с.

17. Абалмазов Э.И. Направленные микрофоны: мифы и реальность // «Специальная техника» №4, 1996 г.

18. Хорев А.А. Технические каналы утечки акустической (речевой) информации. «Специальная техника» №1, 1998 г.

19. Саликов В.Л. Приборы ночного видения: история поколений // «Специальная техника», №2, 2000.

20. Волков В.Г. Наголовные приборы ночного видения // «Специальная техника», №5, 2002.

21. Специализированная информационная система «Техника для спецслужб» <http://www.sis-tss.ru>.

22. Бюро научно-технической информации <http://www.bnti.ru>.

23. Агентство технической безопасности «Нимрод» <http://www.nimrod.ru/>

24. Власов К.В., Бобров А.Л. Основы вихретокового неразрушающего контроля Учебное пособие Сибирский государственный университет путей сообщения Новосибирск, 2015. 53 с.

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

26. Специальная техника органов внутренних дел: Часть 1. Учебник / под общ. Ред. Ю.А. Агафонова. – Краснодар: КрУ МВД России, 2011. – 245 с.

27. Сошинов А. Г. Преобразователи неэлектрических величин: Учеб. пособие / ВолгГТУ, Волгоград, 2002. – 36 с.

28. Физические основы измерений: учебное пособие / А. И. Сюрдо, Д. Ю. Бирюков – Екатеринбург: УрФУ 2013. 143 с.

Оглавление

Введение.....	3
1. Методы и средства защиты проводных каналов передачи информации.....	6
1.1. Понятие и классификация технических каналов утечки информации.....	6
1.2. Утечка информации при передаче ее по проводным каналам связи.....	8
1.3. Технические каналы утечки акустической информации....	11
1.4. Способы контроля проводных линий связи и подавления проводных подслушивающих устройств.....	14
1.5. Контрольные вопросы.....	30
2. Методы и средства защиты информации от утечки за счет побочных электромагнитных излучений и наводок.....	32
2.1. Защита информации от утечки за счет побочных электромагнитных излучений и наводок.....	32
2.2. Пассивные методы защиты от утечки за счет ПЭМИН...	35
2.3. Активные меры защиты информации от утечки за счет ПЭМИН.....	37
2.4. Линейное зашумление.....	39
2.5. Пространственное зашумление.....	41
3. Технический контроль эффективности мер защиты информации.....	44
3.1. Контроль характеристик электромагнитного поля.....	44
3.2. Способы и средства обнаружения каналов утечки информации.....	50
3.3. Требования, предъявляемые к минимальному набору специальной аппаратуры контроля.....	54
3.4. Нелинейные радиолокаторы.....	57
3.5. Инженерно-техническая укрепленность охраняемых объектов.....	59
3.5. Контрольные вопросы.....	63
Заключение.....	65
Литература.....	66

Учебное издание

Еськов Александр Васильевич
Победа Александр Сергеевич
Руденко Максим Юрьевич
Гайфулин Виктор Валерьевич

**ФИЗИЧЕСКИЕ ОСНОВЫ ОБРАЗОВАНИЯ ТЕХНИЧЕСКИХ
КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ**

Учебное пособие

В авторской редакции
Компьютерная верстка *Г. А. Артемовой*

ISBN 978-5-9266-1920-8



Подписано в печать 04.12.2023. Формат 60х84 1/16.
Усл. печ. л. 4,0. Тираж 70 экз. Заказ 207.

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