Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Кафедра защиты информации

Л. М. Лыньков, Л. Л. Утин

АКТИВНЫЕ СРЕДСТВА ЗАЩИТЫ ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНЫХ МАШИН

Методическое пособие
по дисциплине «Технические средства обнаружения и подавления каналов утечки информации»
для студентов специальности 1-98 01 02 «Защита информации в телекоммуникациях»
дневной формы обучения

Минск БГУИР 2012

УДК 004.056.5(076)
ББК 32.973.26-018.2я73
Л88

Р е ц е н з е н т ы:
главный научный сотрудник государственного учреждения
«Научно-исследовательский институт
Вооруженных Сил Республики Беларусь»,
доктор технических наук, профессор Э. Г. Лазаревич;

начальник кафедры автоматизированных систем управления войсками
учреждения образования «Военная академия Республики Беларусь»,
кандидат технических наук, доцент А. В. Хижняк

Лыньков, Л. М.

Л88 Активные средства защиты электронно-вычислительных машин : метод. пособие по дисц. «Технические средства обнаружения и подавления каналов утечки информации» для студ. спец. 1-98 01 02 «Защита информации в телекоммуникациях» днев. формы обуч. / Л. М. Лыньков, Л. Л. Утин. – Минск : БГУИР, 2012. – 51 с.
ISBN 978-985-488-756-2.

Рассмотрены теоретические и прикладные вопросы применения активных средств защиты электронно-вычислительных машин.

УДК 004.056.5(076)
ББК 32.973.26-018.2я73

ISBN 978-985-488-756-2

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В результате возросшего за последнее десятилетие спроса на средства защиты электронно-вычислительных машин (далее – ЭВМ) появилось большое количество производителей, предлагающих разнообразные устройства снижения вероятности утечки конфиденциальной информации. Предлагаемые средства отличаются не только массогабаритными характеристиками, но и концептуальными подходами фирм-производителей к защите информации. Особое место среди многообразия средств защиты занимают активные средства защиты, которым и посвящается данное методическое пособие.

Актуальность рассмотрения данного вопроса обусловлена возросшим вниманием к защите информации от несанкционированного ознакомления, модификации (изменения отдельных данных) и утраты (хищения, искажения с потерей смысла, уничтожения), что подтверждается множеством научных трудов. Кроме того, обеспечение защищенности выделенных помещений от утечки информации по различным техническим каналам является необходимой задачей реализации мероприятий по регламентированной защите объектов. Наиболее сложно задача защиты решается в случаях, если выделенные помещения расположены в одном здании со сторонними организациями, когда смежные с защищаемым помещения не контролируются. Подобные случаи достаточно распространены, особенно в условиях аренды помещений несколькими организациями в крупных офисных зданиях.

В данном пособии авторы постарались рассмотреть теоретические и практические вопросы, связанные с применением только активных средств защиты в объеме, необходимом для подготовки специалистов по защите информации в телекоммуникациях.

1. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ, ИСПОЛЬЗУЕМЫЕ ПРИ ПРИМЕНЕНИИ АКТИВНЫХ СРЕДСТВ ЗАЩИТЫ ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНЫХ МАШИН

1.1. Цель, задачи и способы применения активных средств защиты электронно-вычислительных машин

Активные средства защиты ЭВМ применяются с целью нарушения работы или снижения эффективности применения средств перехвата информации путем создания дополнительного электромагнитного поля в защищаемом помещении. Под защищаемым помещением будем понимать объект информатизации, предназначенный для проведения мероприятий, в ходе которых циркулирует конфиденциальная речевая информация и(или) используются стационарные или переносные ЭВМ, обрабатывающие защищаемую информацию [1]. Как правило, активные средства защиты используют в том случае, если применение организационных мер и пассивных средств не обеспечивает выполнение установленных норм защиты или их применение невозможно. В некоторых случаях допускается применение активных средств защиты ЭВМ в комплексе с организационными мерами и пассивными средствами.

Указанная цель может быть достигнута путем решения следующих задач (рис. 1.1).

1. Увеличение уровня шумов на границе контролируемой зоны и в местах потенциального размещения средств перехвата информации до величин, обеспечивающих невозможность выделения информационного сигнала. Под контролируемой зоной понимают территорию вокруг объекта информатизации, на которой исключено неконтролируемое пребывание посторонних лиц и транспортных средств, не имеющих разрешения на постоянный или разовый доступ на объект [1].

2. Формирование ложных (неинформативных) излучений, обеспечивающих дезинформацию средств получения информации.

Основными способами решения данных задач являются (см. рис. 1.1):

– создание маскирующей заградительной шумовой помехи в широком спектре частот;

– формирование маскирующих прицельных по частоте помех;

– применение имитирующих (речеподобных) помех.

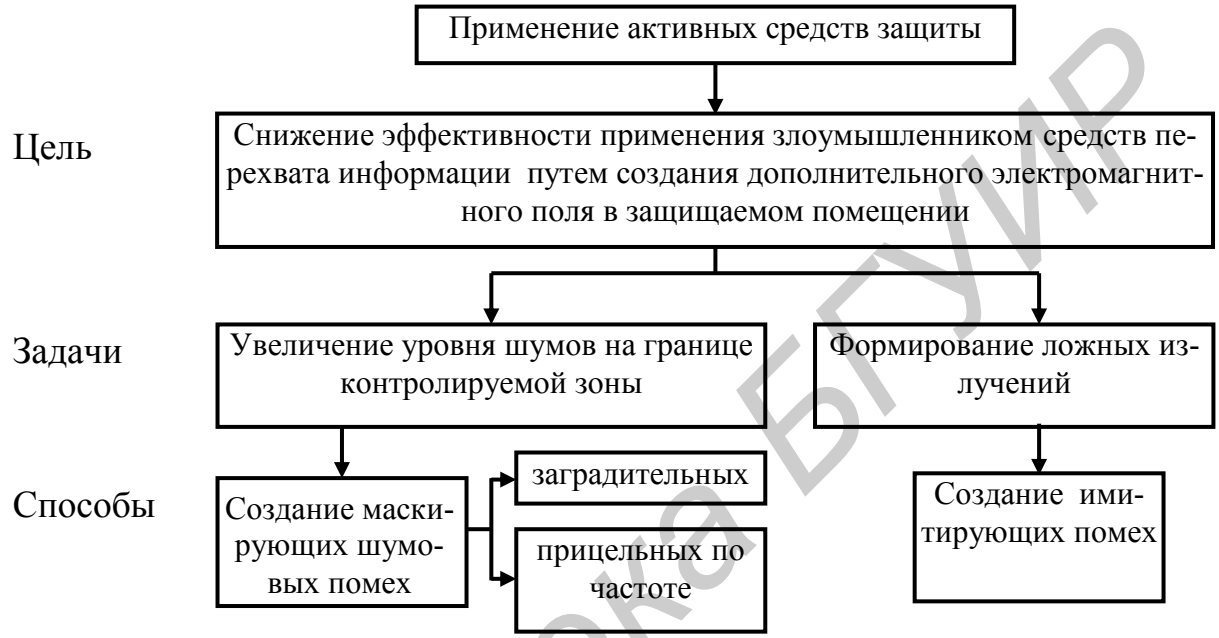


Рис 1.1. Цель, задачи и способы применения активных средств защиты

Для реализации указанных способов формирования электромагнитного поля на практике используют различные средства активной защиты, представляющие собой устройства, формирующие маскирующую заградительную (прицельную) по частоте шумовую помеху или ложную (имитирующую или речеподобную) в заданной пространственной зоне или в линейных проводниках, выходящих за пределы контролируемой зоны.

Для эффективного применения активных средств защиты необходимо знать и учитывать характеристики излучаемых сигналов, особенности их распространения внутри и за пределами защищаемого помещения, характеристики генераторов шума и используемых ими антенн.

1.2. Общие сведения об аналоговых сигналах, циркулирующих в защищаемом помещении

Сигналы, циркулирующие в помещении и подлежащие защите, могут быть аналоговыми и цифровыми. Аналоговым сигналом называется сигнал, амплитуда которого во времени изменяется постепенно (рис.1.2). Примером аналогового сигнала, циркулирующего в защищаемом помещении, является человеческая речь.

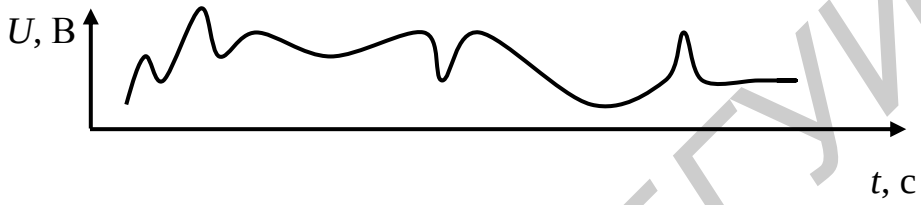


Рис. 1.2. Внешний вид аналоговых сигналов

Речевая информация несет эмоциональную окраску личностного отношения к озвучиваемому сообщению, позволяет не только оперативно перехватывать сведения, требуемые злоумышленнику, но и производить идентификацию личности говорящего. Речевая информация представляет собой акустические колебания в упругой среде. Утечка речевой информации возможна:

– по воздушной среде непосредственно от органов речи человека;

– в результате преобразования звука электрическими устройствами, обладающими микрофонным эффектом (микрофоны, телефоны, громкоговорители, пьезоэлементы и т. д.);

– в результате преобразования акустических сигналов в колебания упругих сред ограждающих конструкций, находящихся внутри выделенных помещений;

– в виде электромагнитных излучений случайных источников (паразитных генераторов), модулированных звуковым сигналом.

В общем случае речевая информация представляет собой сложный частотно- и амплитудно-модулированный шумовой процесс, характеризующийся

частотным диапазоном, разборчивостью и уровнем речевого сигнала. Рассмотрим данные параметры.

Частотный диапазон речи человека лежит в пределах от 150 до 8500 Гц. Последний предел превышают лишь составляющие формантной полосы звука «Ф», которые лежат в области 12 000 Гц. Однако энергия акустических колебаний в пределах рассматриваемого диапазона распределяется неравномерно. Наибольший энергетический уровень речевой информации лежит в пределах 300…3400 Гц, что и позволяет считать эту полосу частот вполне достаточной для обеспечения хорошей разборчивости речи. Форманты в данном диапазоне расположены не только вплотную друг к другу, но и перекрываются.

Под **разборчивостью** речевого сообщения (W) понимают величину, численно равную отношению количества правильно принятых элементов речи ($N_{\text{пр}}$) (формант, звуков, слогов, слов или фраз) к общему количеству передаваемых элементов $N_{\text{пер}}$ [2]:

$$W = \frac{N_{\text{пр}}}{N_{\text{пер}}}. \qquad (1.1)$$

Известно, что по спектральному составу звуки речи различаются числом формант и их расположением в частотном спектре. В результате разборчивость зависит прежде всего от того, какая часть формант дошла до уха человека без искажений, а какая исказилась. Речевой сигнал можно рассматривать как развивающийся во времени процесс, в ходе которого происходит наложение гармонической и формантной структуры. Динамика перестройки формантной структуры определяет смысловое содержание речевого сообщения.

Различные звуки имеют разное число формант: гласные – до 4, глухие согласные – до 5–6. Большинство же звуков речи имеет одну или две форманты, определяющие смысловое содержание речевого сообщения, что обусловлено участием в образовании звуков основных резонаторов голосового аппарата – полости глотки и носоглотки. Первые две форманты называются основными,

остальные – вспомогательными. Основные форманты определяют произносимый звук речи, а вспомогательные – характеризуют индивидуальную для каждого человека окраску, тембр речи [3].

Исключение из передачи любой из формантных областей, как правило, вызывает искажение передаваемого звука, превращая его в другой звук либо приводя к потере им признаков звука человеческой речи.

Исследования показывают, что между формантной, звуковой, слоговой, словесной и фразовой разборчивостью существует тесная взаимосвязь. Учитывая, что речевые сообщения обрабатываются мозгом человека, каждый из перечисленных видов разборчивости требует учета индивидуальных способностей слухового аппарата и логического восприятия людей. В общем случае формантная, звуковая и слоговая разборчивости в большей степени зависят от слухового восприятия человека, чем от логического восприятия. Словесная и фразовая разборчивости зависят от априорных знаний злоумышленником темы речевого сообщения и его продолжительности, логических способностей восстановления целого слова (фразы) по обрывкам слогов (слов), а также избыточности того языка, на котором осуществляется передача информации. Так, для русского языка избыточность равна 60 %, для английского 50 %. В связи с эти справедливо неравенство

$$W_{\text{формант}} < W_{\text{звуков}} < W_{\text{слогов}} < W_{\text{слов англ}} < W_{\text{слов русск}} < W_{\text{фраз}}.$$

Пространство, в котором происходит распространение акустических колебаний, принято называть акустическим полем, направление распространения акустических колебаний – акустическим лучом, а поверхность, соединяющую все смежные точки поля с одинаковой фазой колебания частиц среды – фронтом волны.

В ходе экспериментальных исследований соотношения разборчивости речи и качества приема речевого сообщения определена следующая зависимость (табл. 1.1)[2].

Таблица 1.1

Соотношения между качеством приема речи и ее разборчивостью

Оценка качества приема речевого сообщения	Разборчивость речи	
	Русский язык	Английский язык
Идеально	0,99	1
Отлично	0,98	0,99
Хорошо	0,93	0,98
Удовлетворительно	0,87	0,93
Предельно допустимо	0,75	0,87
Срыв	0,6	0,75
Невозможно восстановить сообщение	0,4	0,5

Уровни речевых сигналов зависят от особенностей речевого аппарата человека и в процессе озвучивания одного сообщения могут изменяться в значительных пределах (табл. 1.2).

Таблица 1.2

Значения уровней различных речевых сигналов

Тип речевой информации	Уровень сигнала, дБ
Тихий шепот	35…40
Спокойная беседа	55…60
Выступление без микрофона	65…70

1.3. Общие сведения о цифровых сигналах, циркулирующих в защищаемом помещении

Цифровым сигналом называется сигнал, амплитуда которого в течение определенного периода времени остается постоянной, а затем в течение малого интервала времени изменяется на постоянную величину и снова остается постоянной (рис. 1.3).

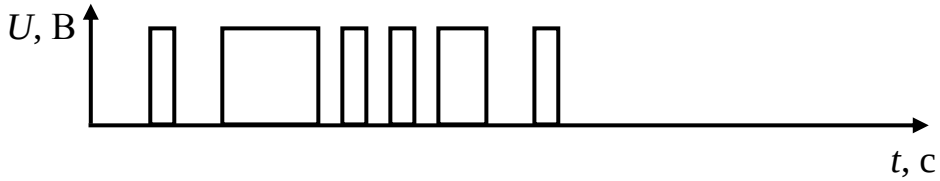


Рис. 1.3. Внешний вид цифровых сигналов

Примерами цифровых сигналов, подлежащих защите, являются:

– сигналы, передаваемые от контроллера клавиатуры к порту ввода–вывода на материнской плате ПЭВМ;

– видеосигналы от видеоадаптера до электродов электронно-лучевой трубки мониторов;

– сигналы цепей, формирующих шину данных системной шины ПЭВМ;

– сигналы, передаваемые от контроллера манипулятора графической информации к порту ввода–вывода на материнской плате;

– сигналы цепей, формирующих шину данных внутри микропроцессора;

– сигналы синхронизации;

– сигналы с внутренних цепей блока питания компьютеров;

– сигналы аппаратных прерываний;

– сигналы цепей формирования шины управления;

– сигналы цепей формирования адресной шины.

Первые три типа сигналов передаются последовательным кодом, в результате чего обладают низкой защищенностью от утечки по различным техническим каналам. Остальные сигналы передаются параллельным кодом, что затрудняет их перехват.

При оценке качества перехвата цифрового сигнала используют вероятность искажения (битов) информации или вероятность искажения кодовой комбинации.

При определении вероятности ошибочного приема элементов сигнала ($P_{ош}$) характеризует долю ошибочно принятых элементов ($N_{ош}$) от общего числа переданных и определяется по формуле

$$P_{ош} = \frac{N_{ош}}{N}. \qquad (1.2)$$

На практике перехват отдельного элемента цифрового сигнала в большинстве случаев не позволяет осуществить его восстановление. Например, перехвачен один бит из пересылаемой одиннадцатиразрядной комбинации сигнала от контроллера клавиатуры к порту ввода - вывода на материнской плате ПЭВМ. Для того чтобы восстановить сигнал, используют зависимость качества перехваченного цифрового сигнала от вероятности искажения кодовой комбинации (табл. 1.3).

Таблица 1.3

Соотношения между качеством приема цифровых сигналов и вероятностью искажения кодовой комбинации

Оценка качества приема цифрового сообщения	Вероятность искажения кодовой комбинации
Низкое	0,9
Среднее	0,7…0,9
Высокое	0,7…0,1

1.4. Краткая характеристика технических каналов утечки аналоговой и дискретной информации из защищаемого помещения

Под **техническим каналом утечки информации** понимают совокупность объекта защиты информации (его физического проявления), среды распространения излученных (отраженных) этим объектом опасных сигналов различной физической природы, а также технического средства разведки, с помощью которого может добываться информация, подлежащая защите (рис. 1.4).

Рис. 1.4. Технический канал утечки информации

Технические каналы утечки информации можно классифицировать следующим образом (рис. 1.5).

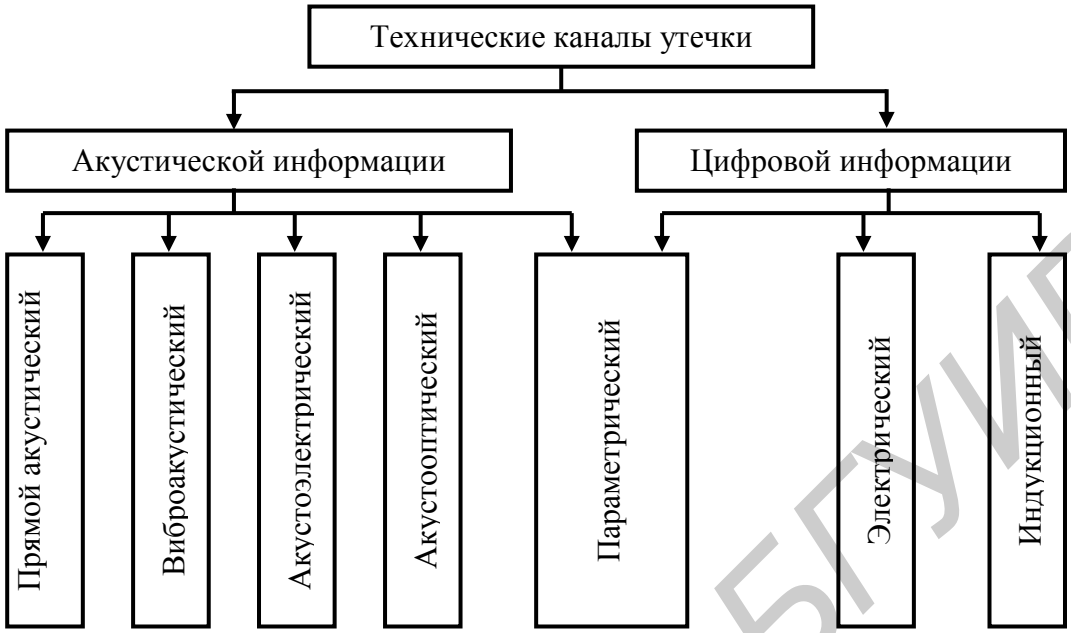


Рис. 1.5. Классификация технических каналов утечки информации

Прямой акустический канал – канал, по которому информация может быть перехвачена путем подслушивания человеком или с использованием направленных микрофонов.

В **виброакустическом канале** утечка информации возможна из-за возникающих под действием акустического сигнала вибраций в ограждающих строительных конструкциях (стенах, потолке, полу) и инженерных коммуникациях (трубах отопления, вентиляции, водоснабжения) защищаемого помещения. Для перехвата информации по данному каналу используют микрофоны твердой среды (виброметры и акселерометры).

Акустоэлектрический канал утечки информации обусловлен изменением под действием акустического сигнала электрических параметров отдельных элементов (емкость, индуктивность, сопротивление) как основных, так и вспомогательных технических средств и систем. Под вспомогательными техническими средствами и системами понимают технические средства и системы, их коммуникации, не предназначенные для обработки конфиденциальной информации, но устанавливаемые на объекте в защищаемом помещении или в поме-

щениях, где размещен объект средств вычислительной техники (электрочасы, электрозвонок, факс, телевизор, радиоприемник, громкоговоритель, датчики охранной и пожарной сигнализации и т. д.) [1]. Под основными техническими средствами и системами понимают технические средства и системы, их коммуникации (информационные кабели, кабели электропитания, заземления), которые входят в состав объекта информатизации и используются для обработки конфиденциальной информации [1].

Акустооптический канал утечки речевой информации образуется при приеме отраженного от вибрирующих окон лазерного луча, промодулированного по амплитуде и фазе акустической волной, циркулирующей в защищаемом помещении.

Параметрический канал утечки как акустической, так и цифровой информации возникает при облучении технических средств передачи информации акустической волной или побочными электромагнитными колебаниями и наводками, вследствие чего возникает переизлучение электромагнитного сигнала.

Побочные электромагнитные излучения и наводки (токи и напряжения в токопроводящих элементах) вызваны электромагнитным излучением, емкостными и индуктивными связями, возникающими при обработке цифровой информации на ЭВМ. В основе появления данных излучений лежат физические явления различного характера, но тем не менее они рассматриваются как канал непреднамеренной передачи информации.

Электрический канал утечки информации связан с наводками электромагнитных излучений на соединительных линиях и посторонних проводниках вспомогательных технических средств, выходящих за пределы контролируемой зоны. Под посторонними проводниками понимают провода, кабели, токопроводящие конструкции, не относящиеся к основным и вспомогательным техническим средствам и системам, размещенным на объектах информатизации

(например, транзитные провода и кабели, трубы систем отопления, водоснабжения, металлоконструкции здания и т. д.) [1].

В **индукционном канале** используется эффект возникновения вокруг кабелей связи электромагнитного поля при прохождении по нему информационных электрических сигналов.

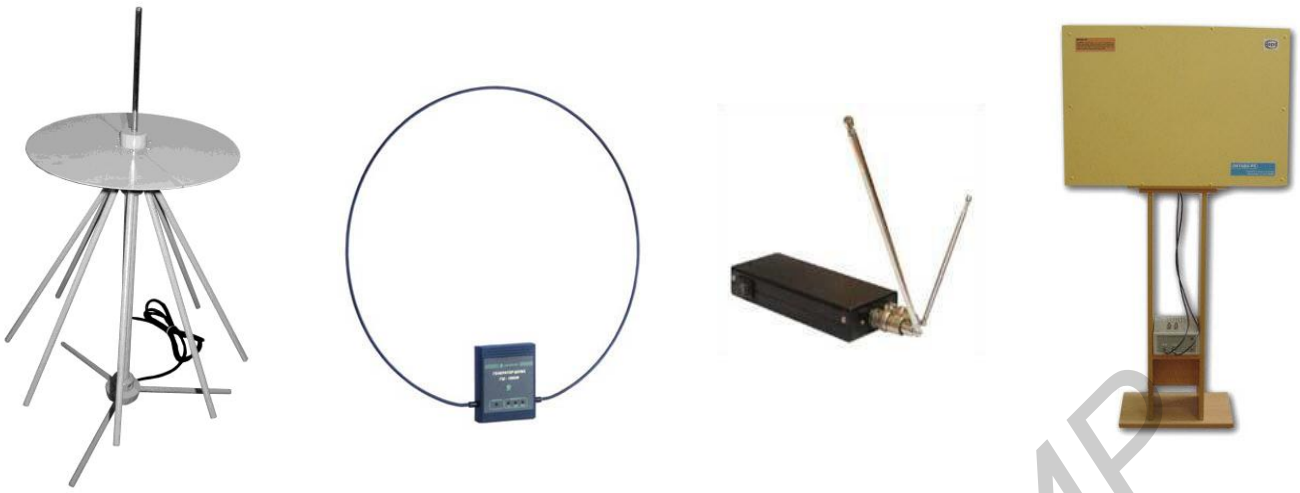
1.5. Общие сведения об антеннах, используемых в защищаемом помещении

На рис. 1.4 видно, что одной из составных частей технического канала утечки информации является антенна. В общем случае под антенной понимается проводник, используемый для излучения или улавливания электромагнитной энергии из окружающей среды. Как правило, в защищаемом помещении рассматриваются случайные антенны, представляющие собой технические средства обеспечения объекта информатизации, их цепи, а также посторонние проводники, способные принимать побочные электромагнитные излучения.

Случайные антенны бывают распределенными и сосредоточенными. Под распределенными случайными антеннами понимают случайные антенны с распределенными электрическими параметрами: провода, кабели, металлические трубы и другие токопроводящие конструкции [1]. Под сосредоточенными случайными антеннами понимают технические средства, измерительную аппаратуру, электронную оргтехнику, средства вычислительной техники, телефонные аппараты, громкоговорители радиотрансляционной сети и др. [1].

Кроме случайных антенн в защищаемом помещении могут находиться и другие типы антенн, например, используемые с активными средствами защиты ЭВМ (рис. 1.6).

Основными характеристиками антенн являются диаграмма направленности, поляризация и коэффициент усиления.



а б в г

Рис. 1.6. Типы антенн активных средств защиты ЭВМ:
а – «Гром ЗИ-4А»; б – ГШ 2500 М; в – «Баррикада»; г – «Октава-РС»

Диаграмма направленности антенны – это зависимость излучающих свойств антенны от пространственных координат. Одна из наиболее простых диаграмм направленности соответствует изотропной антенне, под которой понимают точку в пространстве, излучающую энергию одинаково во всех направлениях (рис. 1.7).

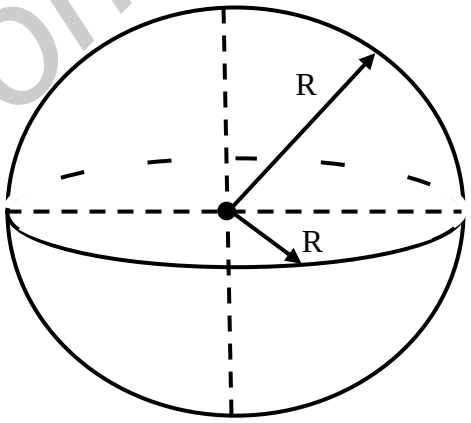
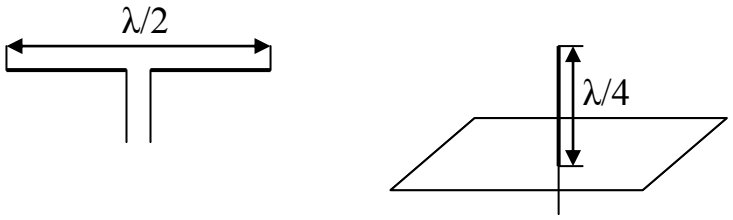


Рис. 1.7. Внешний вид диаграммы направленности изотропной антенны

Учитывая, что размеры ЭВМ значительно меньше расстояния до точки возможного перехвата информации, можно при моделировании излучений ЭВМ использовать рассмотренную выше диаграмму направленности.

В качестве антенн активных средств защиты, как правило, применяют полуволновые диполи (вибраторы Герца) или четвертьволновые вертикальные антенны (антенны Маркони) (рис. 1.8).

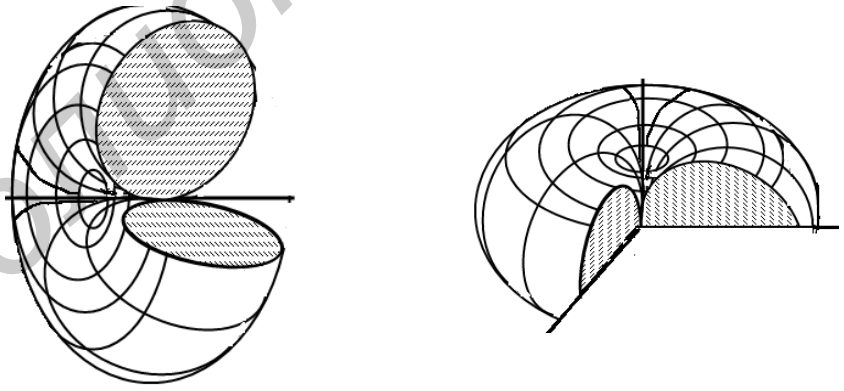


а б

Рис. 1.8. Внешний вид антенн активных средств защиты:
а – полуволновой диполь; б – четвертьволновая антенна

Полуволновой диполь состоит из двух прямых коллинеарных проводников равной длины, разделенных небольшой щелью, на которую подается сигнал. Максимальная эффективность передачи сигнала при использовании антенн данного типа достигается, если размеры антенны равны половине длины волны (λ/2). Полуволновой диполь характеризуется диаграммой направленности, по форме напоминающую сплюснутый тороид (рис. 1.9, а).

Диаграмма направленности антенны Маркони в горизонтальной плоскости имеет форму окружности, а в вертикальных плоскостях – главный максимум излучения (рис. 1.9, б).

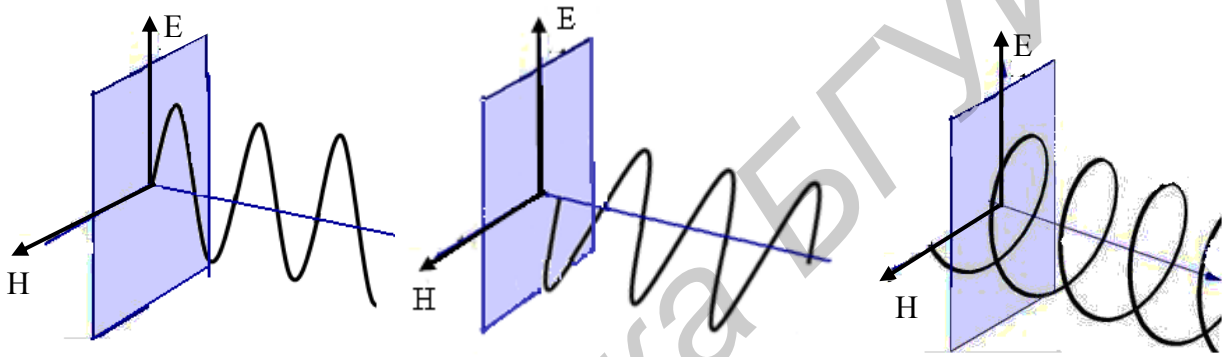


а б

Рис. 1.9. Внешний вид диаграмм направленности:
а – полуволнового диполя; б – четвертьволновой антенны

Диаграммы направленности рассмотренных типов антенн позволяют с успехом использовать их для зашумления сигнала в любом направлении вдоль земной поверхности.

Под **поляризацией антенны** понимают ее пространственно-временную характеристику, определяемую видом траектории, описываемой концом вектора электрического поля в фиксированной точке пространства. В средствах активной защиты используют антенны с вертикальной, горизонтальной и круговой (эллиптической) поляризацией (рис. 1.10).



а б в

Рис. 1.10. Внешний вид поляризаций антенн:
а – вертикальная; б – горизонтальная; в – круговая

Учет поляризации антенн позволяет получить определенные энергетические преимущества при планировании зон зашумления в защищаемом помещении.

Коэффициент усиления – мера направленности антенны, определяемая как отношение мощности сигнала, излученного в определенном направлении, к мощности сигнала, излучаемого антенной в любом направлении. Он определяется в соответствии с выражением

$$G = \frac{4\pi S}{\lambda^2}, \qquad (1.3)$$

где G – коэффициент усиления антенны;

S – эффективная площадь антенны;

λ – длина волны.

Выражения для определения эффективной площади наиболее распространенных типов антенн представлены в табл. 1.4.

Таблица 1.4

Эффективная площадь некоторых типов антенн

Тип антенны	Эффективная площадь, м^2
Изотропная	$\frac{\lambda^2}{4\pi}$
Бесконечно малый диполь или контур	$\frac{1{,}5\ \lambda^2}{4\pi}$
Полуволновой диполь	$\frac{1{,}64\,\lambda^2}{4\pi}$
Рупорная	$0{,}81 \cdot S_{\text{раструба}}$
Параболическая	$0{,}56 \cdot S_{\text{лиц. поверхности}}$
Турникетная (два перпендикулярных диполя)	$\frac{1{,}5\,\lambda^2}{4\pi}$

Длина волны определяется по формуле

$$\lambda = \frac{c}{f}, \qquad (1.4)$$

где c – скорость света ($c \approx 3 \cdot 10^8$ м/с);

f – частота излучаемого сигнала.

1.6. Особенности распространения излучаемых сигналов в защищаемых помещениях

При распространении сигнала в любой среде его интенсивность уменьшается с расстоянием, что связано с потерями мощности в свободном пространстве и затуханием. Кроме того, на сигнал воздействуют различные факторы, искажающие его структуру и затрудняющие правильное восстановление с помощью аппаратуры перехвата. К таким факторам можно отнести воздействие

на сигнал естественных и искусственных шумов, атмосферное поглощение, многолучевое распространение, а также преломление.

Потери мощности в свободном пространстве вызваны рассеиванием электромагнитного сигнала по мере распространении в пространстве. Данный фактор оценивают через отношение мощности излученного сигнала ($P_и$) к мощности полученного сигнала ($P_п$). Для идеальной изотропной антенны потери мощности в свободном пространстве определяются по формуле

$$\frac{P_и}{P_п} = \frac{(4\pi d^2)}{\lambda^2}, \qquad (1.5)$$

где d – расстояние, пройденное сигналом после его излучения в пространство;

λ – длина волны.

Для других типов антенн следует учитывать коэффициенты усиления излучающей антенны ($G_и$) и принимающей антенны аппаратуры перехвата информации($G_п$). С учетом данных коэффициентов усиления выражение (1.5) принимает следующий вид:

$$\frac{P_и}{P_п} = \frac{(4\pi d^2)}{G_и G_п \lambda^2}. \qquad (1.6)$$

Затухание сигнала характеризует постоянные потери интенсивности излученного сигнала в единицу длины. При прохождении сигнала через различные препятствия затухание будет различным (табл. 1.5).

Таблица 1.5

Затухание излучений в различных средах

Тип строительных материалов	Затухание ПЭМИН, дБ
Дерево, гипс, стекло	5...10
Жженый кирпич, плиты из прессшлака	5...35
Бетон с железной арматурой	10...90
Металл, кашированный алюминий	90...100

Из табл. 1.5 видно, что ослабление ПЭМИН, проходящих через экраны, изготовленные из одного и того же материала, может лежать в широких преде-

лах, что обусловлено неравномерностью затухания волн на разных частотах. В табл. 1.6 представлены данные об эффективности экранирования электромагнитных излучений зданиями из различных материалов.

Таблица 1.6

Эффективность экранирования электромагнитного излучения зданиями из различных материалов

Тип здания	Эффективность экранирования ПЭМИН на частотах, дБ		
	100 МГц	500 МГц	1000 МГц
Деревянное здание с толщиной стен 20 см	5...7	7...9	9...11
Кирпичное здание с толщиной стен в 1,5 кирпича	13...15	15...17	16...19
Железобетонное здание с ячейкой арматуры 15х15 см и толщиной стен 16 см	20...25	18...19	15...17

Для определения суммарного коэффициента затухания мощности сигнала ПЭМИН (A_i), излученного на частоте F_j в i-м направлении, осуществляется разбиение пути прохождения сигнала на K+1 участок, где K – количество препятствий на i-м направлении распространения сигнала. Учитывая, что на границе раздела двух сред с различными электрофизическими характеристиками падающая электромагнитная волна претерпевает отражение и преломление, а также частично поглощается в толще материала, предложено коэффициент затухания сигнала ПЭМИН на i-м направлении определять по формуле [1.5]:

$$A_i = A_{\text{спр}} + \sum_{k=1}^{K} (A_{\text{отр1}} + A_{\text{пог}} \cdot d + A_{\text{отр2}})_k , \qquad (1.7)$$

где $A_{\text{спр}}$ – потери мощности сигнала, распространяющегося в свободном пространстве;

$A_{\text{погл}}$ – потери мощности сигнала за счет поглощения (затухания) энергии в толще k-го препятствия;

$A_{отр1}$ – потери мощности сигнала за счет отражения энергии от границ раздела внешняя среда – препятствие;

$A_{отр2}$ – потери мощности сигнала за счет отражения энергии от границ раздела препятствие – внешняя среда;

k=1...K – условный номер препятствия на i-м направлении распространения сигнала;

d – расстояние, которое проходит сигнал в k-м препятствии.

1.7. Основные виды помех, влияющих на прохождение сигнала

Сигнал, излученный источником информации, при своем распространении модифицируется дополнительными нежелательными сигналами, называемыми помехами. Воздействующие на сигнал помехи бывают непреднамеренные и преднамеренные. Классификация непреднамеренных помех представлена на рис 1.11.

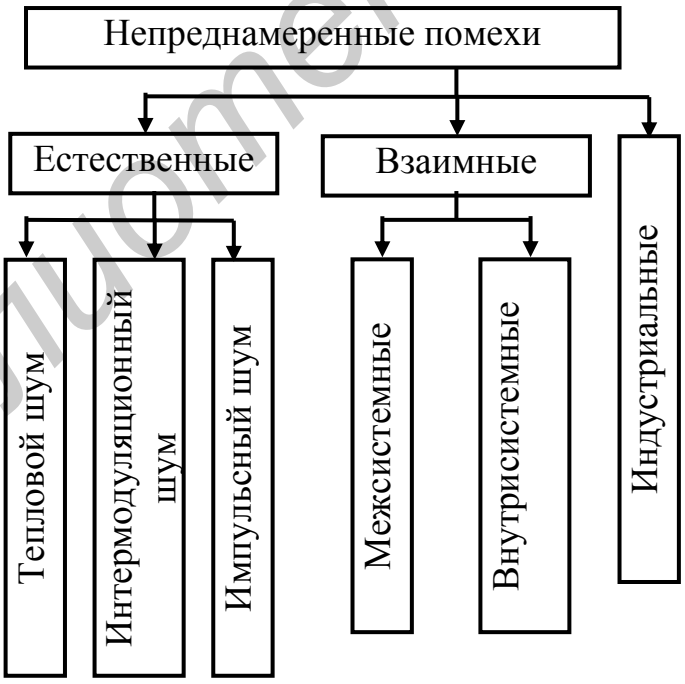


Рис. 1.11. Классификация непреднамеренных помех

Тепловой шум – результат теплового движения электронов, оказывающий влияние на все электрические приборы. Тепловой шум – функция температуры, равномерно распределенная по спектру частот. Данная помеха неустранима и существенно определяет производительность аппаратуры перехвата информации. Плотность мощности теплового шума, присутствующего в полосе частот шириной 1 Гц, определяют по формуле

$$N_0 = kT, \tag{1.8}$$

где k – постоянная Больцмана ($k = 1{,}3803 \cdot 10^{-23}$);

T – абсолютная температура.

Интермодуляционный шум – результат смешивания двух сигналов, передаваемых на различных частотах. Он представляет собой сумму, разность или произведение двух исходных сигналов. Данный вид шумов существенно снижает вероятность перехвата сигнала от ПЭВМ, т. к. съем интермодуляционного сигнала может привести к приему ложной информации разведывательной аппаратурой злоумышленника.

Импульсные шумы – электромагнитная помеха в виде одиночного импульса, последовательности или пачки импульсов с высокой амплитудой. Импульсные шумы возникают из-за молний, неисправностей аппаратуры и множества других причин. Как правило, импульсные шумы незначительно влияют на перехват речевой информации. При перехвате цифровой информации данные помехи приводят к двоичным ошибкам.

Межсистемные помехи – это помехи, источники которых находятся в системе, не относящейся к рассматриваемой.

Внутрисистемные помехи – это электромагнитная помеха, источник которой находится внутри системы.

Индустриальные помехи – это помехи, создаваемые техническими средствами. Источники индустриальных помех весьма многообразны из-за того, что действие любого электромагнитного прибора и устройства сопровожда-

ется электромагнитным излучением. Источники взаимных помех делят на 11 типов (табл. 1.7) [7].

Таблица 1.7

Классификация источников индустриальных помех

Класс индустриальных помех	Источники индустриальных помех
1	Электроустройства различного назначения, эксплуатируемые в жилых домах или подключаемые к бытовой электроосветительной сети
2	Электротранспорт
3	Системы зажигания двигателей внутреннего сгорания
4	Устройства, содержащие источники кратковременных помех
5	Высокочастотные установки промышленного, научного и медицинского назначения
6	Линии электропередач и электрические подстанции
7	Светильники с газоразрядными лампами
8	Электроустройства, питаемые от промышленных энергосистем и эксплуатируемые вне жилых домов
9	Устройства проводной связи
10	Телевизионные и радиовещательные приемники
11	Электроустройства, эксплуатируемые вблизи служебных радиоприемных установок

Преднамеренные помехи – это помехи, которые создаются с помощью специализированных устройств, называемых генераторами шума (рис. 1.12). В соответствии с задачами применения активных средств защиты ЭВМ должны обеспечиваться следующие эффекты воздействия:

– маскирование информационных сигналов, выходящих за пределы защищаемого помещения;

– ведение дезинформации злоумышленников.

Указанные эффекты должны обеспечиваться при воздействии активными помехами на приемные устройства средств перехвата информации, используемых злоумышленником. С учетом данных факторов преднамеренные помехи можно классифицировать следующим образом.

Маскирующие помехи – помехи в техническом канале утечки информации, скрывающие информативный сигнал. Примером маскирующей помехи является широкополосный хаотический сигнал с нормальным (гауссовым) распределением вероятностей мгновенных значений.

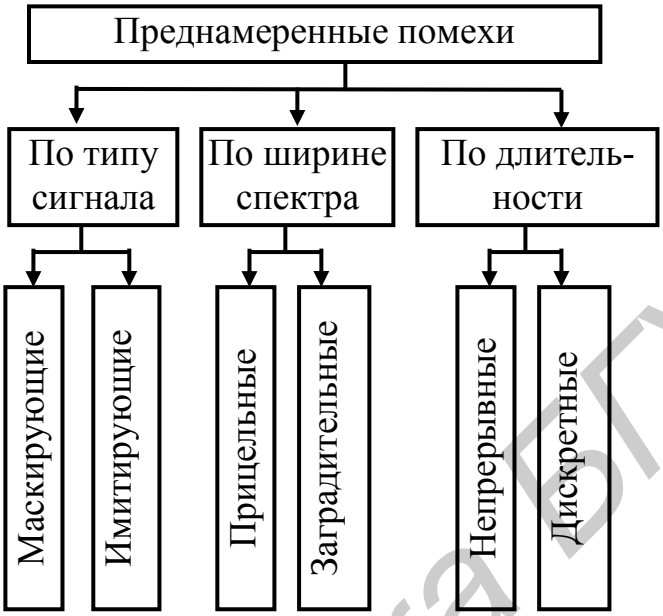


Рис. 1.12. Классификация преднамеренных помех

Имитирующие помехи – тип помех, структура которых подобна структуре основных информативных сигналов, циркулирующих в защищаемом помещении. При планировании применения имитирующих помех их смысловое построение должно соответствовать информации, циркулирующей в защищаемом помещении. Это обусловлено тем, что помехи должны восприниматься аппаратурой перехвата, используемой злоумышленником, как полезная информация. Отсюда следует, что имитирующие помехи должны создаваться активными средствами защиты информации в основном в те интервалы времени, когда конфиденциальная информация в помещениях не обрабатывается. В противном случае целевое назначение имитирующей помехи может быть реализовано только при достаточно больших превышениях помехи над сигналом.

Заградительные помехи – это помехи, перекрывающие весь диапазон частот, в котором предполагается работа аппаратуры перехвата злоумышлен-

ников. Достоинствами заградительной шумовой помехи является формирование электромагнитного поля, вносящего максимальную частотную и структурную неопределенность информативного сигнала для средств перехвата информации. Недостатком данного типа устройств являются большие (по сравнению с устройствами, формирующими прицельные по частоте помехи) энергетические затраты. Кроме того, мощная помеха создает проблемы электромагнитной совместимости эксплуатируемого устройства с системами радиосвязи, телевидения и другими радиоприемными устройствами, которые попадают в зону действия активных средств защиты.

Прицельные помехи – это помехи, ширина спектра которых соизмерима с шириной спектра подавляемого сигнала. Прицельные помехи характеризуются высокой спектральной плотностью мощности, сосредоточенной в узкой полосе частот. Активные средства защиты, применяющие прицельные по частоте помехи, должны формировать многоканальные шумовые, амплитудно-модулированные или частотно-модулированные излучения. Данные устройства позволяют рационально решать вопросы их электромагнитной совместимости с системами радиосвязи телевидения и другими радиоприемными устройствами, которые попадают в зону действия активных средств защиты. Кроме того, энергетические потенциалы формируемого излучения меньше, чем у заградительной шумовой помехи.

Непрерывные помехи – это помехи, уровень которых изменяется непрерывно в течение заданного интервала времени.

Дискретные помехи – это помехи, уровень которых в течение времени меняется по законам дискретной функции.

2. ОСНОВЫ ПОСТРОЕНИЯ АКТИВНЫХ СРЕДСТВ ЗАЩИТЫ ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНЫХ МАШИН

2.1. Принципы построения активных средств защиты электронно-вычислительных машин и основные требования, предъявляемые к ним

Устройства активной защиты ЭВМ используют маскирующие и имитирующие методы активной маскировки информативных сигналов, циркулирующих в защищаемом помещении.

В основу построения маскирующих средств активной защиты положен принцип создания и излучения в окружающее пространство высококачественных шумовых сигналов, создаваемых за счет хаотизации колебаний в динамических системах. Схемы данных устройств близки к схемам классических генераторов сигналов и отличаются от них специально подобранными нелинейными режимами работы активных элементов, а также наличием дополнительных цепей, увеличивающих число степеней свободы автоколебательной системы.

Маскирующие активные средства защиты ЭВМ, как правило, состоят из источника шумового сигнала, усилителя, системы контроля работоспособности, антенной системы и управляемой (регулируемой) линии задержки. Как правило, выход нелинейного усилителя соединяется со своим входом через линию задержки, что позволяет регулировать положение собственных частот генератора шума (рис. 2.1).

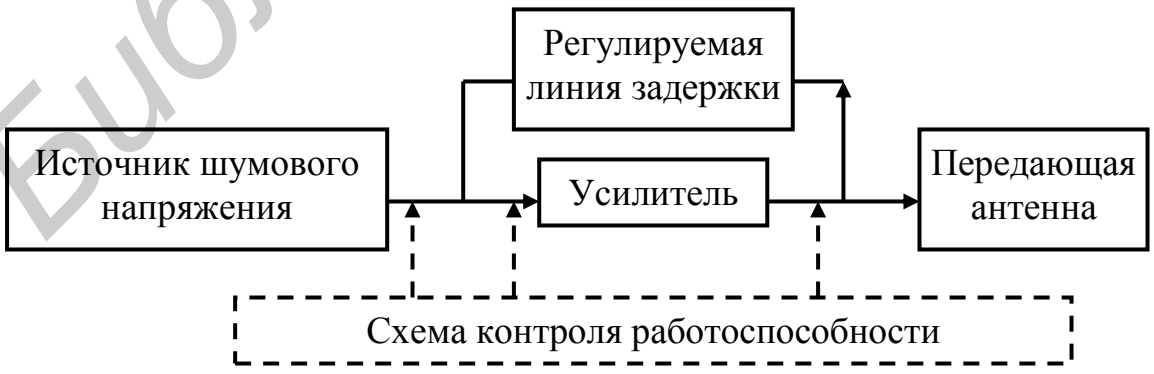


Рис. 2.1. Структурная схема генератора шума

В качестве источника шумового напряжения наиболее часто используют шумовые полупроводниковые диоды, работающие в режиме лавинного пробоя *p*-*n*-перехода.

Временной случайный процесс, близкий по своим свойствам к параметрам шумового сигнала, наиболее целесообразно получать с помощью цифровых генераторов шума, формирующих последовательности двоичных символов, которые называют псевдослучайными.

Встроенные системы контроля работоспособности предназначены для постоянного анализа уровня сформированного шумового сигнала и его качества. При отклонении от нормированных значений система вырабатывает звуковой и световой сигнал ошибки.

В отдельных устройствах активной защиты применяют несколько генераторов шума, соединенных между собой через емкостную связь (рис. 2.2). Первый генератор представляет собой генератор шума с многопетлевой запаздывающей обратной связью и инерционным автосмещением. Данный генератор задает расстановку собственных частот системы и содержит нелинейный усилитель, колебательную систему с распределенными параметрами, цепь запаздывающей обратной связи и инерционную цепь автосмещения. Второй генератор работает в режиме внешнего запуска от первого и содержит нелинейный усилитель, колебательную систему с распределенными параметрами, цепь регулируемой запаздывающей обратной связи.

При создании широкополосных устройств активной защиты ЭВМ учитываются основные факторы, определяющие хаотическую динамику автоколебательных систем вообще и связанных генераторов в частности, таких, как режим работы активного элемента, нелинейность его динамических характеристик и параметры колебательной системы – полоса пропускания, коэффициент обратной связи, инерционность и запаздывание сигнала в цепи обратной связи.

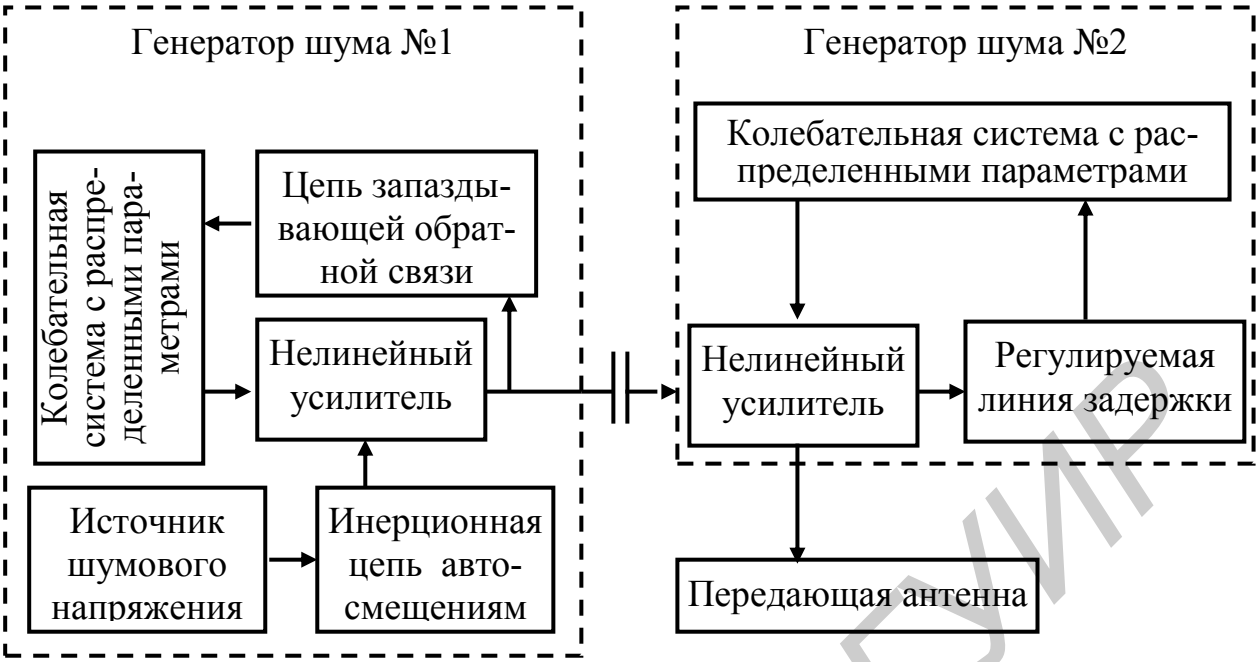


Рис. 2.2. Структурная схема широкополосного генератора шума

Использование двух генераторов шума, объединенных емкостной связью, позволяет:

– расширить частотный диапазон устройств защиты ЭВМ до 2 ГГц;

– сформировать хаотические колебания, не критичные к внешним и внутренним дестабилизирующим факторам (изменению питающего напряжения, температуры, разбросу параметров активных элементов, изменению нагрузки).

Маскирующие активные средства защиты ЭВМ излучают специальный маскирующий сигнал. Как правило, данные устройства компактны и устанавливаются как на корпусе самой ЭВМ, так и в непосредственной близости от нее. Во многих генераторах шума уровень излучаемого маскирующего сигнала не превосходит уровня информативных электромагнитных излучений ЭВМ, поэтому согласования таких средств активной защиты со службой радиоконтроля не требуется.

К устройствам активной защиты ЭВМ предъявляют следующие требования.

1. Устройства должны создавать шумовые электромагнитные помехи в широком диапазоне частот, в котором возможен перехват информации, циркулирующей в защищаемом помещении.

2. Мощность передатчика должна быть достаточной для того, чтобы в точке потенциального перехвата помехи превышали или были бы соизмеримы по мощности с информативным сигналом. Это особенно характерно для речевых сигналов, обладающих повышенной помехоустойчивостью из-за того, что на приемной стороне человеческое ухо может различать полезные сигналы даже при наличии достаточно высокого уровня помех.

3. Диаграмма излучения антенных систем должна быть круговой, что связано с априорной неизвестностью расположения приемной аппаратуры злоумышленника. Если же выяснено вероятное направление перехвата информативного сигнала, целесообразно использование направленных антенн.

4. На границе контролируемой зоны уровень помех, создаваемых активными средствами защиты, не должен превышать требуемых норм по электромагнитной совместимости.

5. Уровень электромагнитных полей, создаваемых генераторами шума на рабочих местах, не должен превышать значений, установленных требованиями санитарных правил и норм Республики Беларусь.

Для формирования имитирующей помехи необходимо генерировать последовательности импульсов, по структуре соответствующие цифровым сигналам, излучаемым ЭВМ. Например, с целью имитации набора текста клавиатуры, осуществляемого при вводе паролей, возможна генерация кодов ASCII. Применение данного типа имитирующей помехи в защищаемом помещении затруднит селекцию истинного сигнала из суммарного электромагнитного поля за требуемое время.

Наиболее эффективное применение имитирующих акустических помех достигается при излучении сигнала, сформированного из фрагментов речи именно тех лиц, которые будут вести переговоры в защищаемом помещении.

2.2. Основные технические характеристики средств маскирования цифровых сигналов

В предыдущем разделе было показано, что генераторы шума представляют собой источник электромагнитных колебаний, спектр которых должен перекрывать частотный диапазон от единиц килогерц до единиц гигагерц, а мощность достаточна для маскировки полезного сигнала. Следует отметить, что до появления методов извлечения полезного сигнала из смеси сигнал плюс помеха генераторы шумов существенно осложняли процесс съема информации за пределами контролируемой зоны. Жесткая конкуренция на рынке средств защиты информации способствовала увеличению энергетических параметров генераторов в широком диапазоне частот и привела к появлению множества типов генераторов, отличающихся не только конструктивно, но и реализующих различные дополнительные возможности.

В настоящее время на рынке можно встретить генераторы шума [6], выполненные в виде автономных блоков и реализованные на платах, вставляемых в слот компьютеров, одноканальные генераторы со встроенными антенными системами и многоканальные, обеспечивающие формирование пространственного электромагнитного шума, излучаемого тремя перпендикулярно расположенными антеннами.

Первым предприятием, наладившим выпуск серийных генераторов шума в Республике Беларусь, явилось частное унитарное предприятие «Завод СВТ». Его изделие **ПАЗК-1** – прибор активной защиты компьютеров (рис. 2.3) – прошло сертификацию в оперативно-аналитическом центре при Президенте Республики Беларусь.

Рис. 2.3. Внешний вид прибора активной защиты компьютеров ПАЗК-1

На рынке технических средств защиты хорошо зарекомендовали себя такие генераторы шума, как **ГШ-1000М, ГШ-К-1000М**. Генератор шума ГШ-1000М (рис. 2.4, а) конструктивно выполнен в пластмассовом корпусе, в котором размещена плата генератора. Антенная система выполнена в виде магнитного диполя (рамка), представляет собой металлический проводник, помещенный в пластиковую изолирующую оболочку, и закреплена к боковым стенкам корпуса. Электропитание генератора шума ГШ-1000М осуществляется напряжением 12 В от сетевого адаптера 220 В/50 Гц. При установке ГШ-1000М на объекте предусмотрен поворот плоскости излучающей антенны вокруг оси, проходящей через боковые стенки корпуса. При этом плоскость антенны можно поворачивать на ±90° и фиксировать в этих пределах под любым углом.

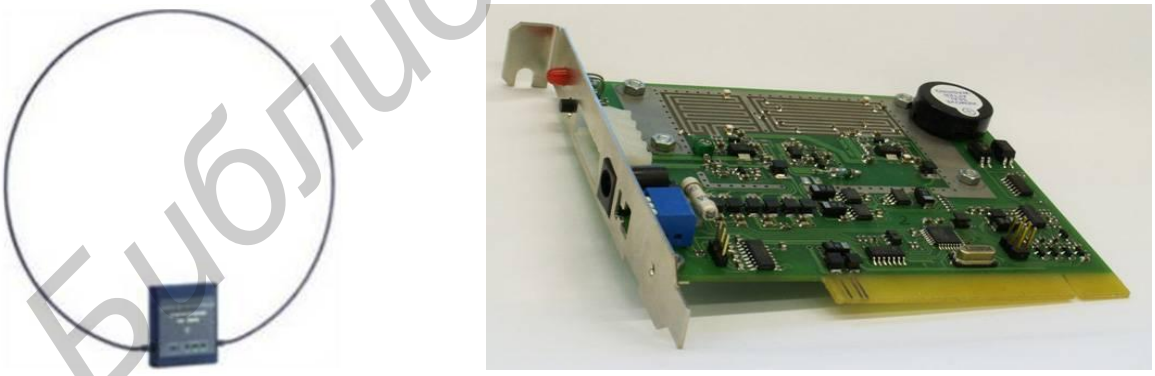
Генератор шума ГШ-К-1000М (рис. 2.4, б) выполнен на печатной плате, которая устанавливается в свободный слот шины PCI или ISA материнской платы персонального компьютера. Антенная система также выполнена в виде магнитного диполя (рамки) и представляет собой гибкий изолированный проводник длиной 1,95 м, закрепленный на металлической планке. При установке ГШ-К-1000М в системный блок персонального компьютера антенна выводится через отверстие в задней стенке и с помощью прилагаемых в комплект поставки диэлектрических распорок ей придается форма окружности. Электропитание генератора осуществляется напряжением 12 В от блока питания компьютера.

а б

Рис. 2.4. Внешний вид генераторов шума:
а – ГШ-1000М; б – ГШ-К-1000М

Некоторые специалисты считают, что данные генераторы не всегда решают поставленные задач по защите помещений от утечки информации из-за низкого уровня шумовых сигналов в диапазоне частот выше 1000 МГц. Кроме того, данным устройствам активной защиты присуща критичность режима формирования шумового маскирующего сигнала к напряжению электропитания, низкий уровень наведенного маскирующего сигнала в цепях электропитания, заземления, инженерных коммуникациях, линиях вспомогательных технических средств связи, включая линии телефонной связи и пожарной сигнализации.

Учитывая, что спектр информативных побочных излучений и наводок современных компьютеров и периферийных устройств может занимать диапазон частот от единиц килогерц до 1800…2000 МГц, в последние годы на рынке предложены модели сверхширокополосных генераторов с хаотической динамикой, обладающих заданными спектральными, статистическими и эксплуатационными характеристиками. Типовым представителем данных моделей являются **ГШ-2500, ГШ-К-1800** (рис. 2.5). Схемное решение этих устройств идентичное, различия заключаются в рабочем частотном диапазоне и конструктивном исполнении.



а б

Рис. 2.5. Внешний вид генераторов шума:
а – ГШ-2500; б – ГШ-К-1800

ГШ-2500 работает в диапазоне частот от 0,1 до 2000 МГц. Конструктивно выполнен в пластмассовом корпусе, в котором размещена плата с двумя гене-

раторами. Первый генератор содержит активный элемент, цепь запаздывающей обратной связи (T = 5,5 нс) и инерционное автосмещение. Интервал между собственными частотами данного генератора составляет приблизительно 180 МГц. Цепь инерционного автосмещения генератора выполнена на пассивных *RC*-элементах. Положение рабочей точки активного элемента данного генератора определяется резистивным делителем напряжения и падением напряжения на элементах инерционного автосмещения, которое зависит от протекающего через транзистор тока, а также соотношений постоянных времени заряда и разряда конденсатора в цепи инерционного автосмещения и времени запаздывания сигнала в цепи обратной связи. Второй генератор выполнен также на транзисторе и содержит между входом и выходом регулируемую цепь запаздывающей обратной связи (T ~ 3,0 нс), выполненную в виде микрополосковой линии. Собственная частота этого генератора может регулироваться в диапазоне частот 270…350 МГц. Связь между генераторами осуществляется с помощью емкостного элемента связи.

Основная антенная система выполнена в виде магнитного диполя (рамка), включенного в коллекторную цепь второго парциального генератора шума, представляет собой металлический проводник, помещенный в пластиковую изолирующую оболочку, и закреплена к боковым стенкам корпуса. Параллельно к этой антенне подключена первая штыревая антенна. К выходу первого парциального генератора также подключена штыревая антенна. Дополнительные штыревые антенны позволяют расширить частотный диапазон устройства радиомаскировки до 2000 МГц. Электропитание генератора шума ГШ-2500 осуществляется напряжением 12 В от сетевого адаптера 220 В/50 Гц.

Близкими по техническим характеристикам к рассмотренным выше средствам активной защиты являются генераторы шума **ЛГШ-501, Волна-4М, SEL SP-21 «Баррикада», Гном 3, Октава-РС, Соната-Р2** (рис. 2.6), характеристики которых представлены в табл. 2.1.

а б в г д е

Рис. 2.6. Внешний вид генераторов шума:
а – ЛГШ-501; б – «Волна-4М»; в – SEL SP-21 «Баррикада»; г – «Гном 3»;
д – «Октава-РС», е – «Соната-Р2»

Отдельно следует рассмотреть генератор шума **ГШ-1000У** (рис. 2.7), работающий в диапазоне частот 0,1…1800 МГц и снабженного четырьмя дополнительными выходами. Конструктивно ГШ-1000У включает пять независимых генераторов шума в одном корпусе. Первый генератор нагружен на излучающую антенну в виде рамки (магнитного диполя) на поворотной оси. К коаксиальному выходу каждого из последующих четырех дополнительных генераторов могут быть подключены дополнительные антенны, улучшающие пространственные и поляризационные характеристики излучаемого электромагнитного поля. Кроме того, к ГШ-1000У можно подключать направленные ответвители, позволяющие наводить маскирующий шум в сети питания, заземления, вспомогательных технических средствах и инженерных коммуникациях.

Рис. 2.7. Внешний вид генератора шума ГШ -1000У

Генератор шума ГШ-1000У оборудован схемой контроля работоспособности, срабатывающей при уменьшении уровня сигнала на выходе генератора ниже определенного порога.

Таблица 2.1

Технические характеристики генераторов шума

Тип (модель) изделия	Наименование характеристик			
	Диапазон частот, МГц	Спектральная плотность шума, дБ	Вид антенны	Конструктивное исполнение
ПАЗК-1	0,01…1000	30…40	Телескопическая	Переносной
ГШ-1000М	0,1…1000	40…75	Рамочная жесткая	Переносной
ГШ-К-1000М	0,1…1000	20…66	Рамочная мягкая	Бескорпусной, вставляется в слот ПЭВМ
ГШ-2500	0,1…2000	27…70	Рамочная жесткая	Переносной
ГШ-К-1800	0,01…1800	32…72	Рамочная мягкая	Бескорпусной, вставляется в слот ПЭВМ
ЛГШ-501	0,01…1800	50…85	Две телескопические	Переносной
Волна-4М	0,01…1000	30…60	Рамочная мягкая	Переносной
SEL SP-21 «Баррикада»	0,1…2000	50…60	Две телескопические	Переносной
«Гном-3»	0,1…1000	38…55	Рамочная мягкая	Стационарный
«Соната Р-2»	0,01…2000	20…40	Встроенная	Стационарный
ГШ-1000У	0,01…1800	35…75	Рамочная жесткая	Переносной

Отдельные предприятия создают не просто генераторы шума, а целые комплексы по защите ЭВМ (табл. 2.2). Например, комплексы **П-220** (рис. 2.8) являются универсальными генераторами шума [9], предназначенными для активной защиты объектов информатизации путем маскирования ПЭМИН шумовыми сигналами.

Данные комплексы позволяют обеспечить зашумление кабелей станционного монтажа и магистральных кабелей; зашумление абонентских и соединительных линий; пространственное зашумление при использовании соответствующих антенн; зашумление цепей электропитания и заземления.

Комплексы конструктивно выполнены по модульному принципу и представляют собой набор генераторов шумов различной мощности, обеспечивающих формирование случайных шумовых сигналов с непрерывным спектром в широком диапазоне частот. В качестве источника шума используются тепловые шумы.

Рис. 2.8. Внешний вид комплекса активной защиты ЭВМ П-220

Базовым блоком комплекса является аппарат ТАФ07 (ТАФ07-1), в который устанавливается блок питания и контроля ТЕИ-13 (ТЕИ13-1) и от 2-х до 10-ти модулей ГШ в следующих комбинациях.

1. Блок ТЕИ14 и блок ТЕИ14-1 представляют собой генераторы шума, состоящие из независимых источников шума и усилителей мощности. Данные блоки предназначены для зашумления двух симметричных и шести несимметричных линий (цепей нагрузки) в кабелях станционного монтажа и магистральных линиях в диапазоне частот от 20 до 10000 Гц с непрерывным спектром.

2. Блок ТЕИ14-2 – широкополосный генератор, предназначенный для зашумления цепей питания, заземления с помощью согласующих устройств типа «трансформатор тока» и пространственного зашумления с использованием соответствующих НЧ- или ВЧ- антенн в диапазоне частот 2…1 500 000 Гц с непрерывным спектром.

3. Блок ТЕИ15 – генератор шума, имеющий в своем составе восемь независимых источников шума с симметричными выходами. Данный блок обеспечивает зашумление абонентских и соединительных линий связи, обеспечивая возможность как симметричного, так и несимметричного подключения.

Еще одним универсальным прибором защиты является устройство активной защиты **Гром-ЗИ-4** и его модификация **Гром-ЗИ-4-А** (рис. 2.9)**.** Данное устройство используется для создания шумовой помехи по радиоканалу, телефонной линии и электросети с целью блокирования несанкционированно установленных передатчиков сигналов.

а б

Рис. 2.9. Внешний вид защитных устройств:
а – Гром-ЗИ-4; б – Гром-ЗИ-4-А

Генератор шума Гром-ЗИ-4-А отличается от других средств активной защиты ЭВМ наличием дискоконусной антенны с квазикруговой диаграммой направленности, которая позволяет формировать шумовую помеху в трех взаимно перпендикулярных плоскостях.

Несмотря на многообразие генераторов шума, практически все они предназначены для работы в режиме постоянного излучения сигнала с уровнем 60 … 80 дБ. По оценкам медицинского персонала электромагнитные излучения такой мощности нарушают обменные процессы и влияют на внутриклеточные изменения в организме людей, могут вызвать развитие лейкемии и других заболеваний. Данные обстоятельства способствовали ужесточению требований по вопросам безопасности и гигиены труда персонала, работающего на ПЭВМ. В результате возникло противоречие между необходимостью использовать мощное излучение для защиты информации, обрабатываемой с использованием ПЭВМ, и требованием по ограничению уровня шумов в помещениях, определенных СН «Шум на рабочих местах. Предельно допустимые уровни» №9-86 РБ 98.

С целью выполнения санитарных норм созданы активные средства защиты с регулируемой мощностью типа SEL SP 113 «Блокада» (рис. 2.10). Излучение маскирующего шумового сигнала осуществляется при помощи двух антенн. Питание устройства осуществляется от внешнего источника питания напряжением 12 В и током не менее 1 А. Устройство имеет световую и звуковую индикацию, указывающую на аварийный режим работы.

Рис. 2.10. Внешний вид средства защиты SEL SP 113 «Блокада»

Таблица 2.2

Технические характеристики комплексов активной защиты

Тип (модель) изделия	Наименование характеристик			
	Диапазон частот, МГц	Спектральная плотность шума, дБ	Вид антенны	Конструктивное исполнение
П-220	0,002…10			Модульный
«Гром-ЗИ-4»	0,1…1000	40…90	Телескопическая	Переносной
«Гром-ЗИ-4-А»	1…1000	40…60	Дискоконусная	Переносной
SEL SP 113 «Блокада»	0,1…1000	40…75	Две телескопические	Переносной
«Соната–РК1»	0,01…1000	30…60	Наружная мягкая	Стационарный

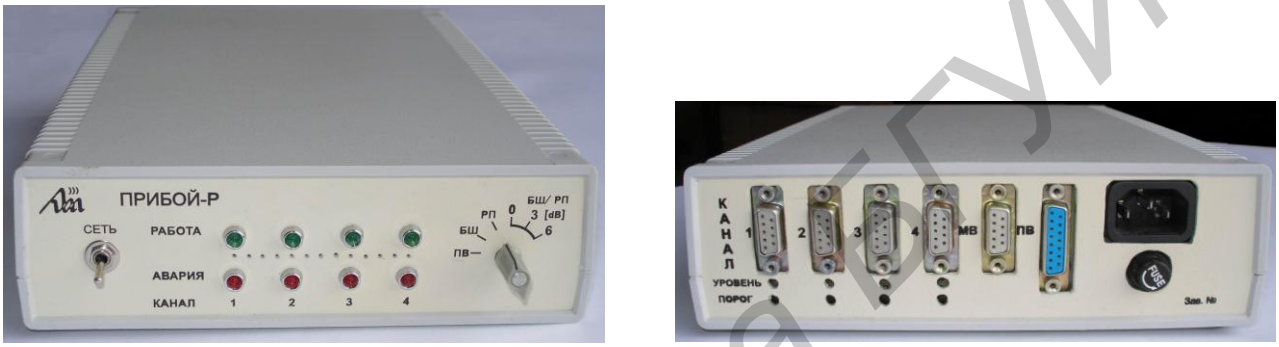
2.3. Устройства активной защиты речевой информации

Устройства активной защиты речевой информации (табл. 2.2), циркулирующей в помещении, предотвращают утечку конфиденциальных сведений по каналам прямого прослушивания, а также при использовании злоумышленником различных микрофонов, стетоскопов и лазерных систем съема информации. Активные средства защиты представляют собой генераторы акустического и виброакустического маскирующего шума, содержащие аудиоизлучатели, виброизлучатели и пьезоизлучатели. Основными видами маскирующего сигнала, формируемого активными средствами защиты, являются белый и розовый шум, а также речевая смесь. Наиболее известными генераторами являются **Прибой-Р**, **Соната–АВ 1М**, **Штора и Шорох**.

Недостаток систем активной защиты речевых сигналов не спасает работающих в помещении людей от чувства дискомфорта из-за назойливых фоновых шумов. Данные шумы вызывают повышенную нервозность и утомляемость персонала, а при длительном воздействии могут приводить к депрессиям и другим функциональным расстройствам нервной системы. Избавиться от возника-

ющего дискомфорта возможно либо снижением мощности генераторов шума, либо самовольным отключением аппаратуры защиты.

Устройство «Прибой-Р» (рис. 2.11), разработанное учреждением образования «Белорусский государственный университет информатики и радиоэлектроники», представляет собой автоматически управляемый источник возбуждения акустических шумов и вибраций, маскирующих речь в элементах конструкции здания. Особенностью генератора шума «Прибой-Р» является его адаптация к голосу человека.



а б

Рис. 2.11. Внешний вид генератора шума «Прибой-Р»:
а – лицевая сторона; б – тыльная сторона

Устройство формирует маскирующие сигналы вида «белый шум», «речеподобные сигналы» и их комбинацию, благодаря чему обеспечивается закрытие каналов утечки речевой информации. «Речеподобные сигналы» формируются по случайному закону, отвечая всем формальным свойствам речи (наличие формантного характера сигналов, частота основного тона, равная частоте основного тона маскируемой речи, паузы между словами) и могут быть адаптированы под конкретного человека. Уровень шума, излучаемый данным генератором, подстраивается под говорящего, речь которого надо защитить. Белый шум, издаваемый «Прибоем», усиливается, ослабевает или вовсе прекращается в зависимости от того, громче или тише стали говорить в помещении или вовсе замолчали. Шумовой фон, издаваемый устройством, еле слышен и не мешает говорящим. В 2011 году разработана модификация устройства «Прибой-Р»,

предназначенная для маскирования арабской речи и получившая название «Прибой-А».

Устройства «Прибой-Р» и «Прибой-А» состоят из акустического генератора шума, выносного пульта, выносного микрофона, акустических преобразователей для окон, акустических преобразователей для стен, акустических преобразователей для коммуникаций водопроводных и отопительных сетей, а также акустических преобразователей для вентиляционных каналов и дверных тамбуров (рис. 2.12).

Рис. 2.12. Внешний вид комплектующих генератора шума «Прибой-Р»

Средством защиты от утечки речевой информации является система вибро- и акустической защиты «Соната-АВ» (рис. 2.13), позволяющая нейтрализовать подслушивания в условиях плохой звукоизоляции помещения; применение радио- и проводных микрофонов, установленных в полостях стен, пола в надпотолочном пространстве, вентиляционных коробах и т. д.; применение лазерных и микроволновых систем съема аудиоинформации с окон и элементов интерьера; применение стетоскопов, установленных на стенах (потолках, полах), трубах водо- (тепло-, и газо-) снабжения) и т. д.

Рис. 2.13. Внешний вид генератора шума «Соната-АВ»

Использование в генераторах «Соната-АВ» цифровых формирователей шума обеспечивает стабильность его основных характеристик. Стойкость заградительной помехи, создаваемой данным генератором, к различным методам ее нейтрализации, обеспечивается большим периодом используемых последовательностей и шумовой загрузкой регистров формирователя при включении питания.

Все генераторные блоки системы имеют входы удаленного беспроводного управления. Для построения системы защиты помещения требуются вибро- и пьезоизлучатели. При наладке устанавливается уровень шумового сигнала, который обеспечивает необходимую степень защиты при минимальном акустическом сигнале помехи в помещении, который практически не влияет на комфортность проведения переговоров.

Аудиоизлучатель АИ-65 (рис. 2.14, а) является специализированным электроакустическим преобразователем и предназначен для возбуждения акустического шума. Конструкция и размеры аудиоизлучателя и элементов его крепления оптимизированы для его установки в надпотолочном пространстве; вентиляционных каналах; дверных тамбурах.

Виброизлучатель ВИ-45 (рис. 2.14, б) является специализированным электромеханическим преобразователем повышенной мощности и предназначен для возбуждения шумовых вибраций в массивных конструкциях защищаемого помещения, обеспечивая при этом приемлемый уровень мешающего акустического шума. Конструкция и размеры виброизлучателя и элементов его крепления оптимизированы для установки на ограждающих конструкциях помещения (стенах, потолках, полах, дверях); массивных окнах (как на рамах, так и на стеклах); трубах систем тепло-, водо- и газоснабжения.

а б в

Рис. 2.14. Внешний вид излучателей, используемых в активных средствах защиты речевой информации:
а – акустоизлучатели; б – виброизлучатели; в – пьезоизлучатели

тромеханическим преобразователем малой мощности и предназначен для возбуждения шумовых вибраций в стеклах окон (дверей, офисных перегородок).

По своим техническим характеристикам близки к рассмотренным выше средствам активной защиты речевой информации следующие генераторы шума: «Штора», «VNG-012GL», комплекс виброакустической защиты «Барон», система виброакустической защиты «ВГШ-103» (рис. 2.15).

При применении средств активной защиты речевой информации следует учитывать, что в настоящее время существуют способы очистки зашумленных речевых сигналов с помощью специальной аппаратуры, в которой реализованы функции распознавания и идентификации речи. В зависимости от класса данных систем время распознавания речи говорящего может осуществляться в масштабе времени, близком к реальному. Поэтому маскирование речевой информации, циркулирующей в защищаемом помещении, должно применяться для защиты только от простого прослушивания.

а

б

в

г

д

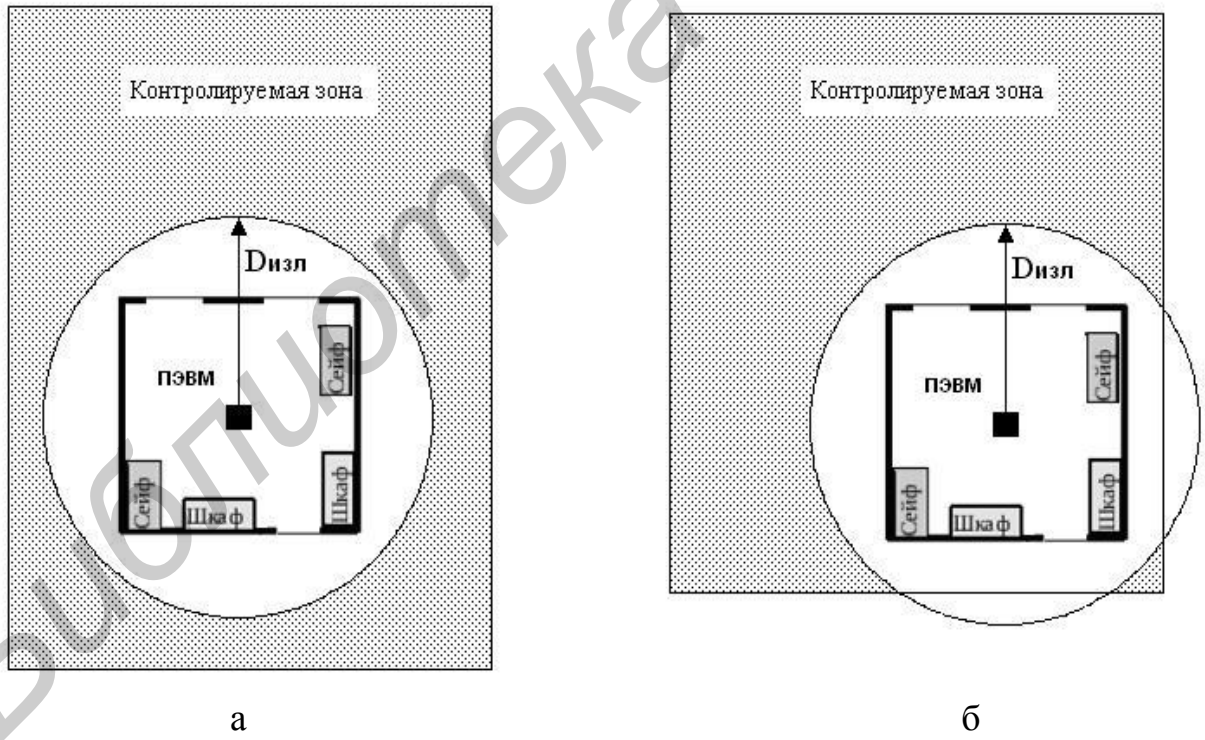
е

Рис. 2.15. Внешний вид средств защиты речевой информации:
а – «Штора-4»; б – «Барон»; в – ВГШ-103; г – VNG-012GL;
д – VNG-006D; е – «Факир»

2.4. Рекомендации по применению активных средств защиты

Средства формирования пространственного (линейного) электромагнитного поля целесообразно применять как дополнительные, если несмотря на все принятые организационные меры и используемые пассивные средства защиты не обеспечиваются требуемые уровни снижения ПЭМИН от ЭВМ в пределах контролируемой зоны, или как основные на временно развертываемых объектах информатизации.

При оценке целесообразности применения активных средств защиты ЭВМ проводят исследования уровней излучений полезного сигнала на границе контролируемой зоны. При проведении данных исследований возможны две ситуации: зона излучения ЭВМ не выходит за пределы контролируемой зоны (рис. 2.16, а) или выходит частично (рис. 2.16, б).



а б

Рис. 2.16. Соотношение размеров контролируемой зоны и дальности изучения информационного сигнала

Из рис. 2.16 видно, что в первом случае установка активных или пассивных средств защиты необязательна, т. к. технические возможности средств об-

наружения электромагнитных излучений не позволят без проникновения на контролируемую территорию осуществить перехват информации. В данном случае в ходе определения политики безопасности следует сделать акцент на организационных и технических мерах по охране контролируемой территории (установка средств наблюдения и сигнализации, периодическая проверка территории на наличие несанкционированных средств съема информации, подбор персонала и др.).

Второй случай является более распространенным. Он характерен для офисных зданий, когда в соседних помещениях размещаются организации, занимающиеся различными сферами деятельности. В таких помещениях установка активных средств защиты обоснована, однако их применение может оказать негативное влияние на здоровье персонала [6]. В этой связи представляется целесообразным проведение исследований контура излучения ЭВМ, находящейся в реальной обстановке функционирования. Результаты подобных исследований дадут возможность определить наиболее опасные направления излучения, на которых необходимо использовать активные средства защиты.

Экспериментальные исследования зон зашумления генераторов шума показывают, что одно устройство активной защиты обеспечивает защиту ЭВМ, размещенных в помещении общей площадью около 40 м^2. Если защищаемое помещение имеет большую площадь, то целесообразно использовать несколько комплектов устройств активной защиты ЭВМ, размещая их по периметру объекта. Максимальное расстояние между соседними устройствами радиомаскировки не должно превышать 20 м.

Активные средства защиты должны создавать электромагнитное помеховое излучение в широком диапазоне частот (0,1…3 ГГц), что обусловлено возможным диапазоном распространения побочных электромагнитных излучений и наводок.

Созданное электромагнитное поле должно распространяться как с вертикальной, так и горизонтальной поляризацией.

Уровень созданных шумовых помех (как по электрической, так и по магнитной составляющей поля) должен обеспечивать на границе контролируемой зоны превышение над уровнем полезных сигналов, а за пределами границы контролируемой зоны не должен превышать требуемых норм по электромагнитной совместимости с системами радиосвязи, телевидения и другими радиоприемными устройствами.

При использовании генераторов шума предпочтение следует отдавать устройствам, имеющим возможность адаптивной подстройки уровня помехи относительно уровня сигнала.

Как правило, установка и включение устройств активной маскировки может быть произведена без каких-либо трудоемких монтажных работ. Устройства активной защиты не требуют квалифицированного обслуживания, их надежная работа гарантируется встроенными схемами контроля работоспособности.

Все устройства активной защиты после хранения в холодном или сыром помещении, а также после транспортировки до включения необходимо выдержать в нормальных условиях не менее 2 часов. Целесообразно использовать помещения без пыли, паров кислот, щелочей, а также газов, вызывающих коррозию.

Не рекомендуется использовать активные средства защиты на борту воздушных, морских и речных судов, при следовании железнодорожным транспортом, т. к. создаваемые шумовые сигналы могут нарушить радиосвязь и управление этими транспортными средствами.

Не допускается механическое повреждение изоляции сетевого кабеля сетевого адаптера, а также попадание на него химически активных компонентов (кислот, масла, бензина и т. п.). При включенных устройствах не рекомендуется касаться телескопических антенн, т. к возможно получение легких ожогов.

Не рекомендуется использовать активные средства защиты ЭВМ в непосредственной близости от радио- и телевизионных устройств во избежание сбоев в их работе.

ЛИТЕРАТУРА

1. Сборник основных терминов и определений в области защиты информации : справ. пособие. – Минск : НИИ ВС РБ, 2010. – 100 с.

2. Основы радиоэлектронной борьбы в ракетных войсках / В. А. Бабуль [и др.]. – Минск : УО «ВА РБ», 2000. – 386 с.

3. Дворянкин, С. В. Обоснование критериев эффективности защиты речевой информации от утечки по техническим каналам / С. В. Дворянкин, Ю. К. Макаров, А. А. Хореев // Защита информации INSIDE. – 2007. – №2. – С. 23 – 25.

4. Утин, Л. Л. Особенности оценки утечек информации через побочные электромагнитные излучения и наводки / Л. Л. Утин, Х. М. Кред // Инженерный вестник. – 2010. – №2(30). – С. 27 – 31.

5. Утин, Л. Л. Усовершенствованная методика построения зоны излучения персональных электронных вычислительных машин / Л. Л. Утин, В. Л. Григорьев, Х. М. Кред // Доклады БГУИР. – 2010. – №7(53). – С. 53 – 58.

6. Утин, Л. Л. Оптимизация размещения средств активной защиты специальной вычислительной техники / Л. Л. Утин, Х. М. Кред. // Тез. докл. междунар. науч.-техн. конф., Минск, 19 марта 2009. – Минск, БГУИР, 2009. – С. 176 – 177.

7. Практикум инженера. Источники индустриальных электромагнитных помех. [Электронный ресурс]. – 2011. – Режим доступа: http://www.vxi.su. – Дата доступа 02.2011.

8. Прибор активной защиты компьютеров ПАЗК-01 [Электронный ресурс]. – 2011. – Режим доступа: http://www.zsvt.by. – Дата доступа 02.2011.

9. Технические средства и методы защиты информации : учебник для вузов / А. П. Зайцев [и др]; под ред. А. П. Зайцева. – М. : ООО «Издательство Машиностроение», 2009. – 508 с.

Св. план 2011, поз. 92

Учебное издание

Лыньков Леонид Михайлович

Утин Леонид Львович

АКТИВНЫЕ СРЕДСТВА ЗАЩИТЫ ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНЫХ МАШИН

Методическое пособие
по дисциплине «Технические средства обнаружения и подавления каналов утечки информации»
для студентов специальности 1-98 01 02 «Защита информации в телекоммуникациях»
дневной формы обучения

Редактор Н. В. Гриневич
Корректор Е. Н. Батурчик
Компьютерная верстка Ю. Ч. Клочкевич

Подписано в печать 04.01.2012.	Формат 60x84 1/16.	Бумага офсетная.
Гарнитура «Таймс».	Отпечатано на ризографе.	Усл. печ. л. 3,14.
Уч.-изд. л. 2,7.	Тираж 100 экз.	Заказ 249.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
ЛИ №02330/0494371 от 16.03.2009. ЛП №02330/0494175 от 03.04.2009.
220013, Минск, П. Бровки, 6