**ОГЛАВЛЕНИЕ**

Введение…………………………………………………………………………...2

Анализ объекта защиты………………………………………………………......4

Расчет контролируемой зоны объекта…………………………………………...7

Выявление каналов утечки и несанкционированного доступа к ресурсам….10

Возможные каналы утечки информации ……………………………………...15

Планирование защитных мероприятий по видам дестабилизирующего воздействия………………………………………………………………………30

Составление плана ТЗИ на объекте…………………………………………….40

Обеспечение ИБ выделенного объекта………………………………………...44

Стетоскопы……………………………………………………………………….73

Заключение………………………………………………………………………..75

Список литературы………………………………………………………………76

ВВЕДЕНИЕ

С древнейших времен любая деятельность людей основывалась на получении и владении информацией, т.е. на информационном обеспечении. Именно информация является одним из важнейших средств решения проблем и задач, как на государственном уровне, так и на уровне коммерческих организаций и отдельных лиц. Но так как получение информации путем проведения собственных исследований и создания собственных технологий является достаточно дорогостоящим, то часто выгоднее потратить определенную сумму на добывание уже существующих сведений. Таким образом, информацию можно рассматривать как товар. А бурное развитие техники, технологии и информатики в последние десятилетия вызвало еще более бурное развитие технических устройств и систем разведки. В создание устройств и систем ведения разведки всегда вкладывались и вкладываются огромные средства во всех развитых странах. Сотни фирм активно работают в этой области. Серийно производятся десятки тысяч моделей «шпионской» техники. Этому во многом способствуют недостатки правовой базы Украины. Хотя в последнее время органы власти уделяют вопросам защиты информации более пристальное внимание. Эта отрасль бизнеса давно и устойчиво заняла свое место в общей системе экономики Запада и имеет под собой прочную законодательную базу в отношении как юридических, так и физических лиц, т.е. строго регламентирована и реализована в четко отлаженном механизме исполнения.

Тематики разработок на рынке промышленного шпионажа охватывают практически все стороны жизни общества, безусловно, ориентируясь на наиболее финансово-выгодные. Спектр предлагаемых услуг широк: от примитивных радиопередатчиков до современных аппартно-промышленных комплексов ведения разведки. Конечно, у нас нет еще крупных фирм, производящих технику подобного рода, нет и такого разнообразия ее моделей, как на Западе, но техника отечественных производителей вполне может конкурировать с аналогичной западной, а иногда она лучше и дешевле. Естественно, речь идет о сравнении техники, которая имеется в открытой продаже. Аппаратура же, используемая спецслужбами (ее лучшие образцы), намного превосходит по своим возможностям технику, используемую коммерческими организациями.

Все это связано с достаточным риском ценности разного рода информации, разглашение которой может привести к серьезным потерям в различных областях (административной, научно-технической, коммерческой и т.д.). Поэтому вопросы защиты информации (ЗИ) приобретают все более важное значение.

Целью несанкционированного сбора информации в настоящее время является, прежде всего - коммерческий интерес. Как правило, информация разнохарактерна и разноценна и степень ее секретности (конфиденциальности) зависит от лица или группы лиц, кому она принадлежит, а также сферы их деятельности. Бизнесмену, например, необходимы данные о конкурентах: их слабые и сильные стороны, рынки сбыта, условия финансовой деятельности, технологические секреты. А в политике или в военном деле выигрыш иногда оказывается просто бесценным, т.к. политик, администратор или просто известный человек является информантом. Интересны его уклад жизни, связи в определенных кругах, источники личных доходов и т.д. А развитие деловых отношений определяет сегодня резкое возрастание интереса к вопросам безопасности именно речевой информации. Особенностью защиты речевой информации является то, что она не материальна, поэтому защищать ее чисто техническими средствами сложнее, чем секретные документы, файлы и другие носители информации.

В процессе зарождения новых проектов и заключения выгодных соглашений непрерывно растет число деловых контактов. При этом любая процедура принятия решения подразумевает, прежде всего, речевое общение партнеров. По данным аналитиков, работающих в области безопасности, удельный вес речевой информации может составлять до 80 % в общем объеме конфиденциальных сведений и конкуренты или недоброжелатели могут в своих корыстных целях использовать полученную конфиденциальную информацию. Ее знание может позволить им оперативнее и эффективнее решать такие проблемы, как: избежать деловых отношений с недобросовестным партнером, пресечь готовящиеся невыгодные действия, шантаж. Т.е. решать проблемы наиболее коротким и быстрым путем. В такой обстановке ни один бизнесмен или руководитель не может чувствовать себя спокойно и быть уверенным в том, что его секреты надежно защищены, несмотря на все многообразие аппаратуры противодействия.

В данной курсовой работе рассматриваются проблемы организации защиты кабинета руководителя от НСД, а также анализируются возможные действия злоумышленника направленные на дестабилизацию целостности, конфиденциальности, доступности информации. Кроме этого, рассматриваются основные методы противодействия от дестабилизирующих факторов, а также даётся оценка эффективности их применения.

**1.Анализ объекта защиты.**

Объект защиты представляет собой кабинет руководителя который

расположен на втором этаже сдания ,с трёх сторон окружён задействованными помещениями в которых расположены разные отделы

организации.за одной из стен (в которой расположено окно) находится улица нас.пункта.Объект предназначен для осуществления управления предприятием, проведение совещаний и переговоров.  
 Краткое описание содержимого комнаты.

Заявляемая категория объекта:

.....3(секретно)  
Этаж: .....2  
Площадь (кв. м), высота потолков (м): *каб. - 48 м2, (6\*8 м), h - 3,30 м*  
- подвесной (воздушный зазор) *потолок гипсолитовый, зазор h - 0,3 м*  
Перекрытия (потолок, пол), толщина (мм): *железобетонные перекрытия*  
Стеновые перегородки: бетон толщина 50 мм   
Стены наружные:*кирпичные*  
- толщина (*73*см)

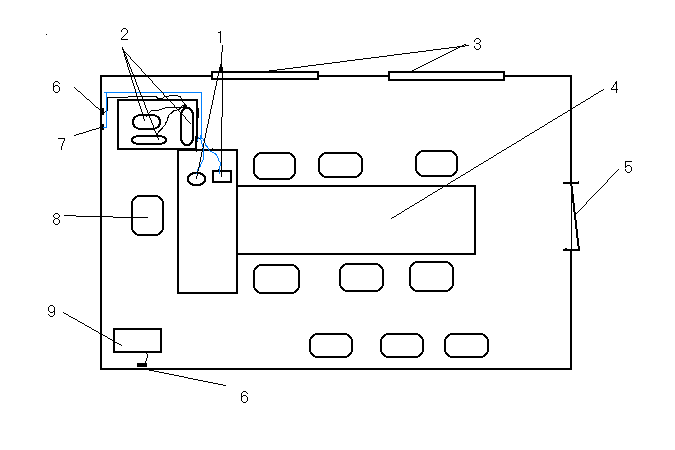
- кирпич *керамический пустотелый*  
- экранирование и штукатурка: *присутствует*  
- другие материалы: *с внутренней стороны стены отделаны под «евростандарт»*

**Окна:**  
- размер проема: .....*200\*80 см*  
- количество проемов: .....*2*  
- наличие пленок (назначение, тип, марка) .....*отсутствуют*  
- тип окна (с двойным утолщенным стеклом): *толщина стекла 6 мм (ОРС 18-15 В)*  
**Двери** :  
- размер проема: *одностворчатые 220\*90 см*  
- двери: *220\*90 см одностворчатые*  
- тип: *легкая одинарная деревянная без уплотнений, замок электронный*  
**Описание смежных помещений:**  
-назначение, характер проводимых работ: *сверху: бухгалтерия, снизу: отдел кадров, север - коридор, юг - трасса, запад - приемная, восток – внешняя стена.*  
-наличие в них технических средств ..... передачи и обработки данных: *ПЭВМ, телефоны.*   
**Система электропитания (освещение):**  
- сеть: *220 В / 50 Гц*  
- тип светильников и их количество: *галогеновые потолочные светильники (6 шт.)*  
**Система заземления:** *имеется*  
Системы сигнализации (тип): *имеется: пожарная (фотооптические детекторы) - 2 шт., охранная (акустические детекторы) - 6 шт.*  
Система вентиляции (тип): *приточно-вытяжная, с мех. побуждением, проем 250\*160 мм*  
**Система отопления:**  
-центральное водяное: *водяное, три стояка, проходящие транзитом снизу вверх*  
- наличие экранов на батареях: *декоративное укрытие*

**Телефонные линии:**  
- количество и тип ТА: .....*2 шт., (Voice Coder-2400- 1 шт), Panasonic - беспроводной 900 МГц )*  
- городская сеть *1 шт., два параллельных аппарата (обычный и беспроводной)*  
- тип розеток: *евророзетка.*  
- тип проводки: *двухпроводные линии, «хлорка»*  
**Оргтехника:** *ПЭВМ в полной конфигурации - 1 шт.*  
**Бытовая техника:**  
- телевизор

* видеомагнитофон   
  **Описание обстановки вокруг объекта:**  
  Объект расположен в центре города, окружен с трех сторон постройками различного назначения и ведомственной принадлежности, с 4-той стороны трассой. Слева от объекта расположено двухэтажное здание, в котором размещен спортивный магазин. Расстояние между зданиями составляет около 10-20 м. Справа от объекта на расстоянии 30-35 м расположен двухэтажный жилой дом.

Схематический план объекта защиты:



1.Телефонные аппараты (обычный и беспроводной).

2.ПК.

3.Окна.

4.Стол для переговоров.

5.Входные двери.

6.Розетки.

7.Телефонная розетка.

8.Место руководителя.

9.Тлевизор, видеомагнитофон.

**2.Расчет контролируемой зоны объекта**

Контролируемая зона – это территория объекта, на которой исключено неконтролируемое пребывания лиц не имеющие постоянного или разового доступа.

Контролируемая зона может ограничиваться периметром охраняемой территорией частично, охраняемой территорией охватывающей здания и сооружения, в которых проводятся закрытые мероприятия, частью зданий, комнаты, кабинеты, в которых проводятся закрытые мероприятия. Контролируемая зона может устанавливаться больше чем охраняемая территория, при этом обеспечивающая постоянный контроль за не охраняемой частью территории. Постоянная контролируемая зона – это зона границы, которой устанавливается на длительный срок. Временная зона – это зона, устанавливаемая для проведения закрытых мероприятий разового характера.

Согласно нормативным документам объекты СО делятся на универсальные объекты, которые в свою очередь делятся на три категории. Согласно требованиям НДТЗИ должна обеспечиваться контролируемая зона следующих размеров.

Первой категории универсального объекта, требуется 50 метров контролируемой зоны. Второй категории объекта, требуется 30 метров, а третей категории объектов требуется 15 метров контролируемой зоны.

Также требуется определенный размер контролируемой зоны для разных типов специализированных объектов таблица №1.

Таблица№1

|  |  |
| --- | --- |
| Тип СО | КЗ (м) |
| 1 | 250 |
| 2 | 100 |
| 3 | 50 |
| 4 | 45 |
| 5 | 40 |
| 6 | 35 |
| 7 | 30 |
| 8 | 20 |
| 9 | 15 |

При выборе мест для размещения объектов необходимо строго

соблюдать требования по обеспечению размера КЗ.

*Требования размеров КЗ по защите перехвата побочных электромагнитных излучений.*

Если на объекте невозможно обеспечить размер КЗ согласно

ДНТЗИ, либо если для размещения отдельной ОТС требуется КЗ

больше чем R то необходимо разделить ОТС на две группы устройств.

1. Устройства прошедшие специальное исследование и удовлетворяющие реальным размерам КЗ объекта.
2. Устройства прошедшие специальное исследование, но не удовлетворяющие реальным размерам КЗ объекта.

Для второй группы необходимо принять дополнительные меры такие как, размещение ОТС в экранированных помещений, кожухах или применение локальных экранов, что обеспечивает защиту в диапазоне частот от 0,15-1000 Мгц.

Требования размеров КЗ по защите от перехвата наводок на вспомогательных технических средствах.

При установки ВТС имеющие выход за пределы КЗ, помещения объектов необходимо обеспечить расстоянием ни менее указанных в нормах ДНТЗИ.

Минимальные допустимые расстояния для универсальных средств.

|  |  |  |  |
| --- | --- | --- | --- |
| Категория универсального  объекта | Минимальные допустимые расстояния до ВТС | | |
| От технических  средств ВТС (м) | От не экранированных  проводов, кабелей ВТС(м) | От экранированных  проводов, кабелей ВТС(м) |
| 1 | 15 | 5,5 | 1,4 |
| 2 | 10 | 3,7 | 0,8 |
| 3 | 5 | 1,8 | 0,5 |

## Минимальные допустимые расстояния по специализированным объектам

|  |  |  |  |
| --- | --- | --- | --- |
| Тип специализированного  объекта | Минимальные допустимые расстояния | | |
| От технических  средств ВТС (м) | От не экранированных  проводов, кабелей ВТС(м) | От экранированных  проводов, кабелей ВТС(м) |
| 1 | 75 | 27,5 | 7,5 |
| 2 | 30 | 11 | 2,7 |
| 3 | 15 | 5,5 | 1,4 |
| 4 | 14 | 5,2 | 1,2 |
| 5 | 12,5 | 4,6 | 1,1 |
| 6 | 11,5 | 4,2 | 1 |
| 7 | 10 | 3,7 | 0,8 |
| 8 | 7 | 2,5 | 0,6 |
| 9 | 5 | 1,8 | 0,5 |

Если на объекте не возможно обеспечить требуемые минимальные расстояния для защиты или если для размещения отдельных ОТС требуется минимальные допустимые расстояния до ОТС, то ОТС делят на две группы устройств:

1. устройства прошедшие специальное исследование и удовлетворяющие реальным, т. е. максимально возможным для данного объекта расстоянием до технических средств и коммутации ВТС имеющий выход за пределы контролируемой зоны.
2. устройства прошедшие специальное исследование и не удовлетворяющие реальным расстояниям до ВТС.

Для устройств второй группы необходимо применять дополнительные меры защиты, которые определяются при помощи ДНТЗИ и на основании категорий и вида объекта.

Поскольку мы не можем обеспечить требуемое минимальное расстояние для защиты за территорией объекта, то мы ограничиваем КЗ стенами кабинета.

**3. Выявление каналов утечки и**

**несанкционированного доступа к ресурсам.**

Сущность защитных мероприятий сводится к перекрытию возможных каналов утечки защищаемой информации, которые появляются в силу объективно складывающихся условий ее распространения и возникающей у конкурентов заинтересованности в ее получении. Каналы утечки информации достаточно многочисленны. Они могут быть как естественными, так и искусственными, т.е. созданными с помощью технических средств.

Перекрытие всех возможных каналов несанкционированногосъема информации требует значительных затрат, и, поэтому, в полном объеме сделать это удается далеко не всегда. Следовательно, в первую очередь необходимо обратить внимание на те из них, которыми с наибольшей вероятностью могут воспользоваться недобросовестные конкуренты.  
наибольшую привлекательность для злоумышленников представляют акустические каналы утечки информации, в особенности такой канал, как виброакустический(за счет распространения звуковых колебаний в конструкции здания).

**Возможные каналы утечки информации**

##### Рассмотрим возможные каналы утечки информациии несанкционированного доступа к ресурсам, которые могут быть использованы противником в данном помещении, а также возможную защиту от них.

Анализ представленных материалов показывает, что в настоящее время номенклатура технических средств коммерческой разведки весьма обширна, что делает задачу надежного блокирования каналов утечки и несанкционированного доступа к информации исключительно сложной.

Решение подобной задачи возможно только с использованием профессиональных технических средств и с привлечением квалифицированных специалистов.

**Основные методы и средства несанкционированного получения информации и возможная защита от них.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **N п/п** | **Действие человека (типовая ситуация)** | **Каналы утечки информации** | **Методы и средства получения информации** | **Методы и средства защиты информации** |
| 1 | Разговор в помещении | * Акустика * Виброакустика * Гидроакустика * Акустоэлектроника | * Подслушивание, диктофон, микрофон, направленный микрофон, полуактивная система * Стетоскоп, вибродатчик * Гидроакустический датчик * Радиотехнические спецприемники | Шумовые генераторы, поиск закладок, защитные фильтры, ограничение доступа |
| 2 | Разговор по проводному телефону | * Акустика * Электросигнал в линии * Наводки | * Аналогично п.1   Параллельный телефон, прямое подключение, электромагнитный датчик, диктофон, телефонная закладка | * Аналогично п.1 * Маскирование, скремблирование, шифрование * Спецтехника |
| 3 | Разговор по радиотелефону | * Акустика * Электромагнитные волны | * Аналогично п.1 * Радиоприемные устройства | * Аналогично п.1 * Аналогично п.2 |
| 4 | Документ на бумажном носителе | Наличие | Кража, визуально, копирование, фотографирование | Ограничение доступа, спецтехника |
| 5 | Изготовление документа на бумажном носителе | * Наличие * Паразитные сигналы, наводки | * Аналогично п.4 * Специальные радиотехнические устройства | * Аналогично п.1 * Экранирование |
| 6 | Почтовое отправление | Наличие | Кража, прочтение | Специальные методы защиты |
| 7 | Документ на небумажном носителе | Носитель | Хищение, копирование, считывание | Контроль доступа, физическая защита, криптозащита |
| 8 | Изготовление документа на небумажном носителе | * Изображение на дисплее * Паразитные сигналы, наводки | * Визуально, копирование, фотографирование * Специальные радиотехнические устройства | Контроль доступа, криптозащита |
| 9 | Передача документа по каналу связи | Электрические и оптические сигналы | Несанкционированное подключение, имитация зарегистрированного пользователя | Криптозащита |
| 10 | Производственный процесс | Отходы, излучения и т.п. | Спецаппаратура различноного назначения, оперативные мероприятия | Оргтехмероприятия, физическая защита |

Таким образом, основным направлением противодействия утечке информации является обеспечение физической(технические средства, линии связи, персонал) и логической (операционная система, прикладные программы и данные) защиты информационных ресурсов. При этом безопасность достигается комплексным применением аппаратных, программных и криптографических методов и средств защиты, а также организационных мероприятий.

Основными причинами утечки информации являются:

• несоблюдение персоналом норм, требований, правил эксплуатации АС;

• ошибки в проектировании АС и систем защиты АС;

• ведение противостоящей стороной технической и агентурной разведок.

Несоблюдение персоналом норм, требований, правил эксплуатации АС может быть как умышленным, так и непреднамеренным. От ведения противостоящей стороной агентурной разведки этот случай отличает то, что в данном случае лицом, совершающим несанкционированные дейст­вия, двигают личные побудительные мотивы. Причины утечки информа­ции достаточно тесно связаны с видами утечки информации.

В соответствии с ГОСТ Р 50922-96 рассматриваются три вида утечки информации:

• разглашение;

• несанкционированный доступ к информации;

• получение защищаемой информации разведками (как отечественны­ми, так и иностранными).

Под *разглашением* информации понимается несанкционированное доведение защищаемой информации до потребителей, не имеющих пра­ва доступа к защищаемой информации.

Под *несанкционированным доступом* понимается получение защи­щаемой информации заинтересованным субъектом с нарушением уста­новленных правовыми документами или собственником, владельцем ин­формации прав или правил доступа к защищаемой информации. При этом заинтересованным субъектом, осуществляющим несанкционированный доступ к информации, может быть: государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное фи­зическое лицо.

*Получение защищаемой информации разведками* может осуществ­ляться с помощью технических средств (техническая разведка) или аген­турными методами (агентурная разведка).

*Канал утечки информации -* совокупность источника информации, материального носителя или среды распространения несущего указанную информацию сигнала и средства выделения информации из сигнала или носителя. Одним из основных свойств канала является месторасположе­ние средства выделения информации из сигнала или носителя, которое может располагаться в пределах контролируемой зоны, охватывающей "АС, или вне ее.

Применительно к АС выделяют следующие каналы утечки:

1. Электромагнитный канал. Причиной его возникновения является электромагнитное поле, связанное с протеканием электрического тока в аппаратных компонентах АС. Электромагнитное поле может индуцировать токи в близко расположенных проводных линиях (наводки). Электромаг­нитный канал в свою очередь делится на следующие каналы:

• радиоканал (высокочастотное излучение);

• низкочастотный канал;

• сетевой канал (наводки на сеть электропитания);

• канал заземления (наводки на провода заземления);

• линейный канал (наводки на линии связи между компьютерными сис­темами).

2. Акустический (виброакустический) канал. Связан с распростране­нием звуковых волн в воздухе или упругих колебаний в других средах, возникающих при работе устройств отображения информации АС.

3. Визуальный канал. Связан с возможностью визуального наблюде­ния злоумышленником за работой устройств отображения информации АС без проникновения в помещения, где расположены компоненты систе­мы. В качестве средства выделения информации в данном случае могут рассматриваться фото-, видеокамеры и т. п.

4. Информационный канал. Связан с доступом (непосредственным и телекоммуникационным) к элементам АС, к носителям информации, к са­мой вводимой и выводимой информации (и результатам), к программному обеспечению (в том числе к операционным системам), а также с подклю­чением к линиям связи. Информационный канал может быть разделен на следующие каналы:

• канал коммутируемых линий связи,

• канал выделенных линий связи,

• канал локальной сети,

• канал машинных носителей информации,

• канал терминальных и периферийных устройств.

* 1. **Возможные каналы утечки информации**

**Утечка акустической информации из-за применения подслушивающих устройств**

Для перехвата и регистрации акустической информации существует огромный арсенал разнообразных средств разведки: микрофоны, электронные стетоскопы, радиомикрофоны или так называемые "радиозакладки", направленные и лазерные микрофоны, аппаратура магнитной записи. Набор средств акустической разведки, используемых для решения конкретной задачи, сильно зависит от возможности доступа агента в контролируемое помещение или к интересующим лицам.   
Применение тех или иных средств акустического контроля зависит от условий применения, поставленной задачи, технических и прежде всего финансовых возможностей организаторов подслушивания.

**Утечка информации за счет скрытного и дистанционного видеонаблюдения**

Из средств данного типа наиболее широко применяются скрыто устанавливаемые фото-, кино-, и видеокамеры с выходным отверстием объектива несколько миллиметров.   
Используются также миниатюрные видеосистемы состоящие из микровидеокамеры с высокой чувствительностью и микрофоном. Устанавливаются на двери или в стене. Для конспиративного наблюдения используются также микровидеокамеры в настенных часах, в датчиках пожарной сигнализации, небольших радиомагнитолах, а также в галстуке или брючном ремне. Видеоизображение может записываться на малогабаритный видеомагнитофон или передаваться с помощью малогабаритного передатчика по радиоканалу в другое помещение или автомашину на специальный или стандартный телеприемник. Расстояние передачи, в зависимости от мощности передачи достигает от 200 метров до 1 км. При использовании ретрансляторов расстояние передачи может быть значительно увеличено.   
Привлекает внимание автомобильная система скрытого видеонаблюдения. Видеокамера, обеспечивающая круговой обзор, закамуфлирована под наружную антенну сотового телефона. Плоский экран устанавливается либо на солнцезащитном козырьке, либо в "бардачке", пульт управления - или в пепельнице, или в кармане на двери. Видеосигнал, в зависимости от комплектации, может записываться прямо на видеомагнитофон либо передаваться по радиолинии на расстояние до 400 м. Видеокамера комплектуется сменными объективами с различными углами зрения.

**Лазерный съем речевой информации**

Для дистанционного перехвата информации (речи) из помещений иногда используют лазерные устройства. Из пункта наблюдения в направлении источника звука посылается зондирующий луч. Зондирующий луч обычно направляется на стекла окон, зеркала, другие отражатели.   
Все эти предметы под действием речевых сигналов циркулирующих в помещении колеблются и своими колебаниями модулируют лазерный луч, приняв который в пункте наблюдения, можно путем несложных преобразований восстановить все речевые сигналы, циркулирующие в контролируемом помещении. На сегодняшний день создано целое семейство лазерных средств акустической разведки. Такие устройства состоят из источника излучения (гелий-неоновый лазер), приемника этого излучения с блоком фильтрации шумов, двух пар головных телефонов, аккумулятора питания и штатива. Наводка лазерного излучения на оконное стекло нужного помещения осуществляется с помощью телескопического визира. Съем речевой информации с оконных рам с двойными стеклами с хорошим качеством обеспечивается с расстояния до 250 метров. Такой возможностью, в частности, обладает система SIPE LASER 3-DA SUPER производства США.   
Однако на качество принимаемой информации, кроме параметров системы оказывают влияние следующие факторы:

* параметры атмосферы (рассеяние, поглощение, турбулентность, уровень фона);
* качество обработки зондируемой поверхности (шероховатости и неровности, обусловленные как технологическими причинами, так и воздействием среды - грязь, царапины и пр.);
* уровень фоновых акустических шумов;
* уровень перехваченного речевого сигнала.

Кроме того, применение подобных средств требует больших затрат не только на саму систему, но и на оборудование по обработке полученной информации. Применение такой сложной системы требует высокой квалификации и серьезной подготовки операторов.   
Из всего этого можно сделать вывод, что применение лазерного съема речевой информации дорогое удовольствие и довольно сложное, поэтому надо оценить необходимость защиты информации от этого вида разведки.

**Пути утечки информации в вычислительных системах**

Вопросы безопасности обработки информации в компьютерных системах пока еще волнуют в нашей стране не слишком широкий круг специалистов.   
До сих пор эта проблема более-менее серьезно вставала у нас, пожалуй, только перед рядом государственных и военных органов, а также перед научными кругами. Теперь же появилось большое число фирм и банков, эффективная деятельность которых практически немыслима без использования компьютеров. Как только должностные лица этих и других организаций это поймут, перед ними сразу же встанут именно вопросы защиты имеющейся у них критичной информации.   
Так что, пока еще есть время, стоит очень серьезно задуматься над имеющимся зарубежным опытом, чтобы не изобретать собственного велосипеда. В частности, для начала небесполезно будет ознакомиться с классификацией и принципами оценивания безопасности компьютерных систем, используемыми в США. Различают два типа некорректного использования ЭВМ:

* доступ к ЭВМ лиц, не имеющих на это права;
* неправильные действия тех лиц, которые имеют право на доступ к ЭВМ (так называемый санкционированный доступ).

Обычно разработчиков систем волнует только решение второй проблемы. Анализ вероятных путей утечки информации или ее искажений показывает, что при отсутствии специальных мер защиты обеспечивающих выполнение функций,возложенных на вычислительную систему, возможно:

* снятие дистанционными техническими средствами секретных сообщений с мониторов ЭВМ, с принтеров (перехват электромагнитных излучений;
* получение информации обрабатываемой в ЭВМ по цепям питания;
* акустическая или электроакустическая утечка вводимой информации;
* перехват сообщений в канале связи;
* навязывание ложного сообщения;
* считывание (изменение) информации ЭВМ при несанкционированном доступе.
* хищение носителей информации и производственных отходов;
* чтение остаточной информации в ЗУ системы после выполнения санкционированных запросов;
* копирование носителей информации;
* несанкционированное использование терминалов зарегистрированных пользователей;
* маскировка под зарегистрированного пользователя с помощью хищения паролей и других реквизитов разграничения доступа;
* маскировка несанкционированных запросов под запросы операционной системы (мистификация);
* использование программных ловушек;
* получение защищаемых данных с помощью серии разрешенных запросов;
* использование недостатков языков программирования и операционных систем;
* преднамеренное включение в библиотеки программ специальных блоков типа "троянских коней";
* злоумышленный вывод из строя механизмов защиты.

В особую группу следует выделить специальные закладки для съема информации с компьютеров.   
Миниатюрный радиомаяк, встроенный в упаковку, позволяет проследить весь путь следования закупленной ЭВМ, транслируя сигналы на специальный передатчик. Узнав таким путем, где установлена машина, можно принимать любую обработанную компьютером информацию через специально вмонтированные электронные блоки, не относящиеся к ЭВМ, но участвующие в ее работе. Самая эффективная защита от этой закладки - экранированное помещение для вычислительного центра.   
По мнению специалистов универсальных "компьютерных закладок" сегодня не бывает. Те закладки, которые удавалось обнаружить, можно условно разделить на три типа: те, которые выбирают информацию по ключевым словам или знакам, те, которые передают всю информацию, находящуюся на винчестере ЭВМ и просто уничтожающие ее.

**Утечка информации за счет ПЭМИН**

Одной из наиболее вероятных угроз перехвата информации в системах обработки данных считается утечка за счет перехвата побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами. ПЭМИН существуют в диапазоне частот от единиц Гц до полутора ГГц и способны переносить (распространять) сообщения, обрабатываемые в автоматизированных системах. Дальность распространения ПЭМИ исчисляется десятками, сотнями, а иногда и тысячами метров. Наиболее опасными источниками ПЭМИН являются дисплеи, проводные линии связи, накопители на магнитных дисках и буквопечатающие аппараты последовательного типа.   
Например с дисплеев можно снять информацию с помощью специальной аппаратуры на расстоянии до 500-1500 метров, с принтеров до 100-150 метров. Перехват ПЭМИН может осуществляться и с помощью портативной аппаратуры. Такая аппаратура может представлять собой широкополосный автоматизированный супергетеродинный приемник. В качестве устройств регистрации принятых сигналов (сообщений) может использоваться магнитный носитель или дисплей.

**Утечка информации при использовании средств связи и различных проводных коммуникаций**

В данном случае, когда речь заходит о возможности перехвата информации при использовании линий связи и проводных коммуникаций, следует иметь в виду, что перехват может осуществляться не только с телефонных линий и не только речевой информации. В этот раздел можно отнести:

* прослушивание и запись переговоров по телефонным линиям;
* использование телефонных линий для дистанционного съема аудио- информации из контролируемых помещений;
* перехват факсимильной информации;
* перехват разговоров по радиотелефонам и сотовой связи;
* использование сети 220 В и линий охранной сигнализации для передачи акустической информации из помещений;
* перехват пейджинговых сообщений.

Рассмотрим кратко каждый из перечисленных каналов утечки информации в отдельности.

**Прослушивание и запись переговоров по телефонным линиям**

Телефонные абонентские линии обычно состоят из трех участков: магистрального (от АТС до распределительного шкафа (РШ)), распределительного (от РШ до распределительной коробки (КРТ)), абонентской проводки (от КРТ до телефонного аппарата). Последние два участка - распределительный и абонентский являются наиболее уязвимыми с точки зрения перехвата информации. Подслушивающее устройство может быть установлено в любом месте, где есть доступ к телефонным проводам, телефонному аппарату, розетке или в любом месте линии вплоть до КРТ.   
Наиболее простой способ подслушивания это подключение параллельного телефонного аппарата или "монтерской" трубки. Используются также специальные адаптеры для подключения магнитофонов к телефонной линии. Адаптеры сделаны таким образом, что диктофон, установленный на запись в режиме акустопуска, включается только при поднятой трубке телефонного аппарата. Это дает возможность экономно расходовать пленку на кассете, не сматывая ее вхолостую.   
гальванически (прямым подсоединением), а и с помощью индукционных или емкостных датчиков. Такое подсоединение практически не обнаруживается с помощью тех аппаратных средств, которые широко используются для поисковых целей.   
Самыми распространенными из подобных средств прослушивания являются телефонные контроллеры радиоретрансляторы которые чаще называются телефонными передатчиками или телефонными "закладками". Телефонные закладки подключаются параллельно или последовательно в любом месте телефонной линии и имеют значительный срок службы, так как питаются от телефонной сети. Эти изделия чрезвычайно популярны в промышленном шпионаже благодаря простоте и дешевизне.   
Большинство телефонных "закладок" автоматически включается при поднятии телефонной трубки и передают разговор по радиоканалу на приемник пункта перехвата, где он может быть прослушан и записан. Такие "закладки" используют микрофон телефонного аппарата и не имеют своего источника питания, поэтому их размеры могут быть очень небольшими. Часто в качестве антенны используется телефонная линия. Для маскировки телефонные "закладки" выпускаются в виде конденсаторов, реле, фильтров и других стандартных элементов и узлов, входящих в состав телефонного аппарата.   
Чаще всего телефонные "закладки" стараются устанавливать за пределами офиса или квартиры, что существенно снижает риск. Для упрощения процедуры подключения подслушивающих устройств и уменьшения влияния на телефонную линию используются изделия с индуктивным датчиком съема информации. Особенностью подобных устройств является то, что требуется автономный источник питания и устройство должно иметь схему автоматического включения при снятии телефонной трубки. Качество перехватываемой информации практически всегда хуже.

**Использование телефонных линий для дистанционного съема аудио- информации из контролируемых помещений.**

Отдельное место занимают системы, которые предназначены не для подслушивания телефонных переговоров, а для использования телефонных линий при прослушивании контролируемых помещений, где установлены телефонные аппараты или проложены провода телефонных линий.   
Примером такого устройства может служить "телефонное ухо". "Телефонное ухо" представляет собой небольшое устройство, которое подключается параллельно к телефонной линии или розетке в любом удобном месте контролируемого помещения. Для прослушивания помещения необходимо набрать номер абонента, в помещении которого стоит "телефонное ухо". Услышав первый гудок АТС необходимо положить трубку и через 10-15 секунд повторить набор номера. Устройство дает ложные гудки занято в течение 40-60 секунд, после чего гудки прекращаются и включается микрофон в устройстве "телефонное ухо" - начинается прослушивание помещения. В случае обычного звонка "телефонное ухо" пропускает все звонки после первого, выполняя роль обычной телефонной розетки и не мешая разговору.   
Кроме того, возможно использование телефонной линии для передачи информации с микрофона, скрытно установленного в помещении. При этом используется несущая частота в диапазоне от десятков до сотен килогерц с целью не препятствовать нормальной работе телефонной связи. Практика показывает, что в реальных условиях дальность действия подобных систем с приемлемой разборчивостью речи существенно зависит от качества линии, прокладки телефонных проводов, наличия в данной местности радиотрансляционной сети, наличия вычислительной и оргтехники и т.д.   
Из числа, так называемых "беззаходовых" систем съема речевой информации с контролируемых помещений, когда используются телефонные линии, следует отметить возможность съема за счет электроакустического преобразования, возникающего в телефонных аппаратах и за счет высокочастотного (ВЧ) навязывания. Но эти каналы утечки используются все реже. Первый из-за того, что современные телефонные аппараты не имеют механических звонков и крупных металлических деталей, а второй из-за своей сложности и громоздкости аппаратуры. Но тем не менее меры защиты от утечки информации по этим каналам применяются, они общеизвестны и не дорогие.

**Использование сети 220 В для передачи акустической информации из помещений.**

Для этих целей применяют так называемые сетевые "закладки". К этому типу "закладок" чаще всего относят устройства, которые встраиваются в приборы, питающиеся от сети 220 В или сетевую арматуру (розетки, удлинители и т.д.). Передающее устройство состоит из микрофона, усилителя и собственно передатчика несущей низкой частоты. Частота несущей обычно используется в диапазоне от 10 до 350 кГц. Передача и прием осуществляется по одной фазе или, если фазы разные то их связывают по высокой частоте через разделительный конденсатор. Приемное устройство может быть изготовлено специально, но иногда применяют доработанные блоки бытовых переговорных устройств, которые сейчас продаются во многих специализированных магазинах электронной техники. Сетевые передатчики подобного класса легко камуфлируются под различного рода электроприборы, не требуют дополнительного питания от батарей и трудно обнаруживаются при использовании поисковой аппаратуры, широко применяемой в настоящее время.

**Рассмотрим подробнее возможности акустического перехвата информации**.

**ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ АКУСТИЧЕСКОЙ (РЕЧЕВОЙ ИНФОРМАЦИИ)**

Под техническим каналом утечки информации (ТКУИ) понимают совокупность объекта разведки, технического средства разведки (TCP), с помощью которого добывается информация об этом объекте, и физической среды, в которой распространяется информационный сигнал. По сути, под ТКУИ понимают способ получения с помощью TCP разведывательной информации об объекте.

Сигналы являются материальными носителями информации. По своей физической природе сигналы могут быть электрическими, электромагнитными, акустическими и т.д. То есть сигналами, как правило, являются электромагнитные, механические и другие виды колебаний (волн), причем информация содержится в их изменяющихся параметрах.

В зависимости от природы сигналы распространяются в определенных физических средах. В общем случае средой распространения могут быть газовые (воздушные), жидкостные (водные) и твердые среды, Например, воздушное пространство, конструкции зданий, соединительные линии и токопроводящие элементы, грунт(земля) и т.п.

Технические средства разведки служат для приема и измерения параметров сигналов.

Под акустической понимается информация, носителем которой являются акустические сигналы. В том случае, если источником информации является человеческая речь, акустическая информация называется речевой.

Акустический сигнал представляет собой возмущения упругой среды, проявляющиеся в возникновении акустических колебаний различной формы и длительности. Акустическими называются механические колебания частиц упругой среды, распространяющиеся от источника колебаний в окружающее пространство в виде волн различной длины.

Первичными источниками акустических колебаний являются механические колебательные системы, например органы речи человека, а вторичными -преобразователи различного типа, в том числе электроакустические. Последние представляют собой устройства, предназначенные для преобразования акустических колебаний в электрические и обратно. К ним относятся пьезоэлементы, микрофоны, телефоны, громкоговорители и другие устройства.

В зависимости от формы акустических колебаний различают простые (тональные) и сложные сигналы. Тональный - это сигнал, вызываемый колебанием, совершающимся по синусоидальному закону. Сложный

сигнал включает целый спектр гармонических составляющих. Речевой сигнал является сложным акустическим сигналом в диапазоне частот от 200...300 Гц до 4…6 кГц. В зависимости от физической природы возникновения информационных сигналов, среды распространения акустических колебаний и способов их перехвата технические каналы утечки акустической (речевой) информации можно разделить на воздушные, вибрационные, электроакустические, оптико-электронный и параметрические.

**ВОЗДУШНЫЕ ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ**

В воздушных технических каналах утечки информации средой распространения акустических сигналов является воздух, и для их перехвата используются миниатюрные высокочувствительные микрофоны и специальные направленные микрофоны.

Миниатюрные микрофоны объединяются (или соединяются) с портативными звукозаписывающими устройствами (диктофонами) или специальными миниатюрными передатчиками. Автономные устройства, конструкционно объединяющие миниатюрные микрофоны и передатчики, называют закладными устройствами перехвата речевой информации, или просто акустическими закладками. Перехваченная закладными устройствами речевая информация может передаваться по радиоканалу, оптическому каналу (в инфракрасном диапазоне длин волн), по сети переменного тока, соединительным линиям вспомогательных технических средств и систем (ВТСС), посторонним проводникам (трубам водоснабжения и канализации, металлоконструкциям и т. п.).Г1ричем для передачи информации по трубам и металлоконструкциям могут использоваться не только электромагнитные, но и механические ультразвуковые колебания

Прием информации, передаваемой закладными устройствами я осуществляется, как правило, на специальные приемные устройства, работающие в соответствующем диапазоне длин волн. Однако встречаются закладные устройства, прием информации с которых можно осуществлять с обычного телефонного аппарата. Такие устройства устанавливаются или непосредственно в корпусе телефонного аппарата, находящегося в контролируемом помещении и называемом "телефоном-наблюдателем", или подключаются к телефонной линии, чаще всего в телефонной розетке.

Подобное устройство конструкционно объединяет миниатюрный микрофон и специальный блок коммутации часто называется "телефонным ухом". Блок коммутации подключает микрофон к телефонной линии придозвоне по определенной схеме до "телефона-наблюдателя" или подаче в линию специального кодированного сигнала. Использование портативных диктофонов и акустических закладок требует проникновения на контролируемый объект (в помещение). В том случае, когда это не удается, для перехвата речевой информации используются направленные микрофоны.

**ВИБРАЦИОННЫЕ ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ**

В вибрационных (структурных) технических каналах утечки информации средой распространения акустических сигналов являются конструкции зданий, сооружений (стены, потолки, полы), грубы водоснабжения, отопления, канализации и другие твердые тела. Для перехвата акустических колебаний в этом случае используются контактные микрофоны (стетоскопы). Контактные микрофоны, соединенные с электронным усилителем, называют электронными стетоскопами. По вибрационному каналу также возможен перехват информации с использованием закладных устройств. В основном для передачи информации используется радиоканал поэтому такие устройства часто называют радиостетоскопами. Возможно использование закладных устройств с передачей информации по оптическому каналу в ближнем инфракрасном диапазоне длин волн, а также по ультразвуковому каналу (по металлоконструкциям здания).

**ЭЛЕКТРОАКУСТИЧЕСКИЕ ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ**

Электроакустические технические каналы утечки информации возникают за счет электроакустических преобразований акустических сигналов в электрические и включают перехват акустических колебаний через ВТСС. обладающие "микрофонным эффектом", а также путем "высокочастотного навязывания".

Некоторые элементы ВТСС. в том числе трансформаторы, катушки индуктивности, электромагнитывторичных электрочасов, звонков телефонных аппаратов, дроссели ламп дневного света, электрореле и т. п " обладают свойством изменять свои параметры (емкость, индуктивность, сопротивление) под действием акустического поля, создаваемого источником акустических колебаний.

Изменение параметров приводит либо к появлению на данных элементах электродвижущей силы (ЭДС). изменяющейся по закону воздействующего информационного акустического поля, либо к модуляции токов, протекающих по этим элементам, информационным сигналом. Например, акустическое поле, воздействуя и на якорь электромагнита вызывного телефонного звонка, вызывает его колебание. В результате чего изменяется магнитный поток сердечника электромагнита. Изменение этого потока вызывает появление ЭДС самоиндукции в катушке звонка, изменяющейся по закону изменения акустического поля. ВТСС, кроме указанных элементов, могут содержать непосредственно электроакустические преобразователи.

К таким ВТСС относятся некоторые датчики пожарной сигнализации, громкоговорители ретрансляционной сети и т.д. Эффект электроакустического преобразования акустических колебаний в электрические часто называют "микрофонным эффектом". Причем из ВТСС, обладающих "микрофонным эффектом", наибольшую чувствительность к акустическому полю имеют абонентские громкоговорители и некоторые датчики пожарной сигнализации. Перехват акустических колебаний в данном канале утечки информации осуществляется путем непосредственного подключения к соединительным линиям ВТСС, обладающих"микрофонным эффектом", специальных высокочувствительных низкочастотных усилителей.

Например, подключая такие средства к соединительным линиям телефонных аппаратов с электромеханическими вызывными звонками, можно прослушивать разговоры, ведущиеся в помещениях, где установлены эти аппараты. Технический канал утечки информации путём "высокочастотного навязывания" может быть осуществлен путем несанкционированного контактного введения токов высокой частоты от соответствующего генератора в линии (цепи), имеющие функциональные связи с нелинейными или параметрическими элементами ВТСС, на которых происходит модуляция высокочастотного сигнала информационным. Информационный сигнал в данных элементах ВТСС появляется вследствие электроакустического преобразования акустических сигналов в электрические.

В силу того, что нелинейные или параметрические элементы ВТСС для высокочастотного сигнала, как правило, представляют собой несогласованную нагрузку, промодулированный высокочастотный сигнал будет отражаться от нее и распространяться в обратном направлении по линии или излучаться. Для приема излученных или отраженных высокочастотных сигналов используется специальные приемники с достаточно высокой чувствительностью. Для исключения влияния зондирующего и переотраженного сигналов могут использоваться импульсные сигналы.

Наиболее часто такой канал утечки информации используется для перехвата разговоров, ведущихся в помещении, через телефонный аппарат, имеющий выход за пределы контролируемой зоны. Для исключения воздействия высокочастотного сигнала на аппаратуру АТС в линию, идущую в ее сторону, устанавливается специальный высокочастотный фильтр .

**ОПТИКО-ЭЛЕКТРОННЫЙ ТЕХНИЧЕСКИЙ КАНАЛ УТЕЧКИ ИНФОРМАЦИИ**

Оптико-электронный (лазерный) канал утечки акустической информации образуется при облучении лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей (стекол окон, картин, зеркал и т.д.). Отраженное лазерное излучение (диффузное или зеркальное) модулируется по амплитуде и фазе (по закону вибрации поверхности) и принимается приемником оптического (лазерного) излучения, при демодуляции которого выделяется речевая информация. Причем лазер и приемник оптического излучения могут быть установлены в одном или разных местах (помещениях). Для перехвата речевой информации по ' данному каналу используются сложные лазерные акустические локационные системы, иногда называемые "лазерными микрофонами". Работают они, как правило в ближнем инфракрасном диапазоне волн.

**ПАРАМЕТРИЧЕСКИЕ ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ**

В результате воздействия акустического поля меняется давление на все элементы высокочастотных генераторов ТСГШ и ВТСС. При этом изменяется (незначительно) взаимное расположение элементов схем, проводов в катушках индуктивности, дросселей и т. п.,, что может привести к изменениям параметров высокочастотного сигнала, например к модуляции его информационным сигналом. Поэтому этот канал утечки информации называется параметрическим. Это обусловлено тем, что незначительное изменение взаимного расположения, например, проводов в катушках индуктивности (межвиткового расстояния) приводит к изменению их индуктивности, а, следовательно, к изменению частоты излучения генератора, т.е. к частотной модуляции сигнала.

Или воздействие акустического поля на конденсаторы приводит к изменению расстояния между пластинами и, следовательно, к изменению его емкости, что, в свою очередь, также приводит к частотной модуляции высокочастотного сигнала генератора. Наиболее часто наблю дается паразитная модуляция информационным сигналом излучений гетеродинов радиоприемных и телевизионных устройств, находящихся в выделенных помещениях и имеющих конденсаторы переменной емкости с воздушным диэлектриком в колебательных контурах гетеродинов.

Промодулированные информационным сигналом высокочастотные колебания излучаются в окружающее пространство и могут быть перехвачены и детектированы средствами радиоразведки. Параметрический канал утечки информации может быть реализован и путем "высокочастотного облучения" помещения, где установлены полуактивные закладные устройства, имеющие элементы, некоторые параметры которых (например, добротность и резонансная частота объемного резонатора) изменяются по закону изменения акустического(речевого)сигнала.

При облучении мощным высокочастотным сигналом помещения, в котором установлено такое закладное устройство, в последнем при взаимодействии облучающего электромагнитного поля со специальными элементами закладки (например, четвертьволновым вибратором) происходит образование вторичных радиоволн, т.е. переизлучение электромагнитного поля. А специальное устройство закладки (например, объемный резонатор) обеспечивает амплитудную, фазовую или частотную модуляцию переотраженного сигнала по закону изменения речевого сигнала. Подобного вида закладки иногда называют полуактивными. Для перехвата информации по данному каналу кроме закладного устройства необходимы специальный передатчик с направленной антенной и приемник.

**ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ АКУСТИЧЕСКОЙ (РЕЧЕВОЙ) ИНФОРМАЦИИ ВОЗДУШНЫЕ**

Перехват акустических сигналов

\* микрофонами, комплексированными с портативными устройствам и звукозаписи

\* направленными микрофонами

\* микрофонами, комплексированными с устройствами передачи информации по радиоканалу

\* микрофонами, комплексированными с устройствами передачи информации по сети электропитания 220В

\* микрофонами, комплексированными с устройствами передачи информации по оптическому каналу в ИК-диапазоне, длин волн.

\* микрофонами, комплексированными с устройствами передачи информации по телефонной линии " микрофонами, комплексированными с устройствами их подключения к телефонной линии ("телефону-наблюдателю") по сигналам вызова от внешнего телефонного абонента

\* микрофонами, комплексированными с устройствами передачи информации по трубам водоснабжения, отопления, металлоконструкциям и т.п.

**ВИБРАЦИОННЫЕ**

Перехват акустических сигналов

\* электронными стетоскопами

\* стетоскопам и, комплексированными с устройствами передачи информации по радиоканалу

\* стетоскопами, комплексированными с устройствами передачи информации по оптическому каналу в ИК-диапазоне длин волн

\* стетоскопами 2 комплексированными с устройствами передачи информации по трубам водоснабжения, отопления, металлоконструкциям и т.п.

**ПОДКУП.**

Это самый простой и эффективный способ получения конфиденциальной информации. Разумеется, он требует некоторой предварительной работы для выяснения степени осведомленности тех или иных сотрудников фирмы в ее делах. Кроме того, подкуп обычно осуществляется через посредников, поэтому необходимым условием является сбор информации о них: надо точно знать, кому дать деньги, сколько, когда, через кого и за что. Однако все издержки такого рода с лихвой перекрываются одним важным обстоятельством — работнику фирмы не требуется преодолевать физические и технические препятствия для проникновения в ее секреты. Значит, остается лишь одно: найти обладателей нужной информации, недовольных своим продвижением по службе, заработком, характером отношений с руководителями, остро нуждающихся в деньгах или просто алчных, готовых ради наживы на любое предательство. Известна грустная статистика (данные Интерпола), согласно которой 25% служащих фирмы готовы продать ее секреты в любое время кому угодно, 50% идут на это в зависимости от обстоятельств и только 25% являются патриотами данного предприятия. Одним из видов подкупа является переманивание ценных специалистов фирмы к себе ради последующего овладения их знаниями. История конкурентной борьбы полна подобных примеров. Для тех 50% сотрудников, которые идут на сотрудничество с конкурентами в зависимости от обстоятельств, необходимые обстоятельства нередко создают через шантаж. Шантаж бывает двух видов. В первом случае человека ловят на крючок, угрожая предать огласке компрометирующие его сведения. Во втором случае, ему просто угрожают мерами физического воздействия (взорвем автомобиль, сожжем дачу, похитим ребенка, изнасилуем дочь или жену, запугаем престарелых родителей и т.д., средств у преступников много).

**ВНЕДРЕНИЕ СВОИХ ЛЮДЕЙ В СОСТАВ ПЕРСОНАЛА КОНКУРИРУЮЩЕЙ ФИРМЫ.**

Тоже представляет распространенный и эффективный способ экономического шпионажа. Для внедрения имеются два пути: первый — когда агент выступает под собственной фамилией и работает в соответствии с имеющейся у него профессией. Второй — когда он трудоустраивается по поддельным документам, под прикрытием легенды. Внедрение собственной агентуры к конкурентам более сложный метод, чем обычный подкуп или шантаж, но, в отличие от завербованных информаторов, свой агент намного надежнее и эффективнее как источник конфиденциальной информации.  
В зависимости от степени ценности информатора строятся и отношения между сотрудничающими сторонами. Чем он важнее, тем больше соблюдается мер конспирации. В частности, встречи с ним маскируются под бытовые контакты, происходят на конспиративных квартирах либо в общественных местах, через тайники и даже с помощью технических средств. Общение с менее ценными людьми может носить обычный характер. При этом стороны особо не заботятся о своей безопасности. Так что выборочное скрытое наблюдение за собственными сотрудниками может дать руководителю фирмы (через его оперативных сотрудников) весьма любопытные сведения для размышлений.

**НАБЛЮДЕНИЕ.**

тоже дает ценную конфиденциальную информацию, особенно если оно сопряжено с копированием документации, чертежей, образцов продукции и т.д. В принципе, процесс наблюдения сложен, так как требует значительных затрат сил, времени и средств. Поэтому его ведут, как правило, выборочно, это значит, в определенном месте, в определенное время, специально подготовленными людьми и с помощью технических средств. Например, волоконно-оптическая система типа РК-1715 имеет кабель длиной до двух метров. Она позволяет проникать в помещения через замочные скважины, кабельные и отопительные вводы, вентиляционные шахты, фальшпотолки и другие отверстия. Угол обзора системы — 65, фокусировка — от 10 км до бесконечности. Работает при слабом освещении. С ее помощью можно читать и фотографировать документы на столах, заметки в настольных календарях, настенные таблицы и диаграммы, считывать информацию с дисплеев. Вообще фотографирование применяется в экономическом шпионаже достаточно широко. Фотосъемка осуществляется с помощью современной аппаратуры при дневном освещении и ночью, на сверхблизком расстоянии и на удалении до нескольких километров, в видимом свете и в инфракрасном диапазоне (в последнем случае можно выявить исправления, подделки, а также прочесть текст на обгоревших документах).  
Современные шпионские фотоаппараты поражают воображение. Так, известны телеобъективы размером всего со спичечный коробок, однако четко снимающие печатный текст на расстояниях до 100 метров! А миниатюрная фотокамера в наручных часах (типа РК-420) позволяет делать 7 кадров на одной кассете с расстояния от одного метра и далее без наводки на резкость, установки выдержки, диафрагмы и прочих тонкостей.  
Большую опасность в плане экономического шпионажа представляют люди, обладающие фотографической зрительной памятью. Им достаточно одного взгляда, чтобы охватить значительное содержание, запомнить и воспроизвести его практически без искажений. Особенно легко это удается специалистам в разведываемой области деятельности, которым достаточно лишь намека, чтобы понять основное содержание текста (чертежа, разработки). Вот пример. Конкурирующая фирма послала на просмотр моделей одежды своего конкурента группу модельеров, каждый из которых специализировался на какой-либо одной детали демонстрируемых моделей: на рукаве, воротнике, спинке и т.д. В условиях строжайшего запрета на фотографирование, видеосъемку, зарисовки и даже на разговоры (чтобы исключить диктовку на магнитофон) они запомнили каждый свои детали. Потом у себя на фирме они восстановили в рисунках все, что видели, по каждой модели!

* 1. **Планирование защитных мероприятий по видам дестабилизирующего воздействия.**

Для защиты от НС доступа который приводит к дестабилизирующему воздействию нужно использовать технические средства защиты информации, и придерживаться правил безопасности.

На этапе проведения организационных мероприятий необходимо:

— определить перечень сведений с ограниченным доступом, подлежащих технической защите (определяет собственник информации в соответствии с действующим законодательством Украины);

— обосновать необходимость разработки и реализации защитных мероприятий с учетом материального или иного ущерба, который может быть нанесен вследствие возможного нарушения целостности ИсОД либо ее утечки по техническим каналам;

— установить перечень выделенных помещений, в которых не допускается реализация угроз и утечка информации с ограниченным доступом;

— определить перечень технических средств, которые должны использоваться как ОТС(основные технические средства);

— определить технические средства, применение которых не обосновано служебной и производственной необходимостью и которые подлежат демонтажу;

— определить наличие задействованных и незадействованных воздушных, наземных, настенных и заложенных в скрытую канализацию кабелей, цепей и проводов, уходящих за пределы выделенных помещений;

— определить системы, подлежащие демонтажу, требующие переоборудования кабельных сетей, цепей питания, заземления или установки в них защитных устройств.

Подготовительные технические мероприятия включают в себя первичные меры блокирования электроакустических преобразователей и линий связи, выходящих за пределы выделенных помещений.

Блокирование линий связи может выполняться следующими способами:

— отключением линий связи ТСПИ и ВТСС или установкой простейших схем защиты;

— демонтажем отдельных технических средств, кабелей, цепей, проводов, уходящих за пределы выделенных помещений;

— удалением за пределы выделенных помещений отдельных элементов технических средств, которые могут являться источником возникновения канала утечки информации.

Блокирование каналов возможной утечки ИсОД в системах городской и ведомственной телефонной связи может осуществляться:

— отключением звонковых (вызывных) линий телефонного аппарата;

— установкой в цепи телефонного аппарата безразрывной розетки для временного отключения;

— установкой простейших устройств защиты.

Предотвращение утечки ИсОД через действующие системы громкоговорящей диспетчерской и директорской связи осуществляется применением следующих защитных мер:

— установкой в вызывных цепях выключателей для разрыва цепей;

— установкой на входе громкоговорителей выключателей (реле), позволяющих разрывать цепи по двум проводам;

— обеспечением возможности отключения питания микрофонных усилителей;

— установкой простейших устройств защиты.

Защита ИсОД от утечки через радиотрансляционную сеть, выходящую за пределы выделенного помещения, может быть обеспечена:

— отключением громкоговорителей по двум проводам;

— включением простейших устройств защиты.

Для службы оповещения следует выделить дежурные абонентские устройства вне выделенных помещений; цепи к этим устройствам должны быть проложены отдельным кабелем.

Предотвращение утечки ИсОД через системы пожарной и охранной сигнализаций осуществляется отключением датчиков пожарной и охранной сигнализации на период проведения важных мероприятий, содержащих ИсОД, или применением датчиков, не требующих специальных мер защиты.

Блокирование утечки ИсОД через системы электронной оргтехники и кондиционирования может быть обеспечено следующими мерами:

— расположением указанных систем внутри контролируемой территории без выноса отдельных компонентов за ее пределы;

— электропитанием систем от трансформаторной подстанции, находящейся внутри контролируемой территории.

При невыполнении указанных выше условий системы должны отключаться от сети электропитания по двум проводам.

Защита ИсОД от утечки через цепи электроосвещения и электропитания бытовой техники должна осуществляться подключением указанных цепей к отдельному фидеру трансформаторной подстанции, к которому не допускается подключение сторонних пользователей.

В случае невыполнения указанного требования электробытовые приборы на период проведения закрытых мероприятий должны отключаться от цепей электропитания.

**Технические мероприятия**

Технические мероприятия являются основным этапом работ по технической защите ИсОД и заключаются в установке ОТС, обеспечении ТСПИ и ВТСС устройствами ТЗИ.

При выборе, установке, замене технических средств следует руководствоваться прилагаемыми к этим средствам паспортами, техническими описаниями, инструкциями по эксплуатации, рекомендациями по установке, монтажу и эксплуатации.

ОТС должны размещаться, по возможности, ближе к центру здания или в сторону наибольшей части контролируемой территории. Составные элементы ОТС должны размещаться в одном помещении либо в смежных.

Если указанные требования невыполнимы, следует принять дополнительные меры защиты:

— установить высокочастотные ОТС в экранированное помещение (камеру);

— установить в незащищенные каналы связи, линии, провода и кабели специальные фильтры и устройства;

— проложить провода и кабели в экранирующих конструкциях;

— уменьшить длину параллельного пробега кабелей и проводов разных систем с проводами и кабелями, несущими ИсОД;

— выполнить технические мероприятия по защите ИсОД от утечки по цепям заземления и электропитания.

К средствам технической защиты относятся:

— фильтры-ограничители и специальные абонентские устройства защиты для блокирования утечки речевой ИсОД через двухпроводные линии телефонной связи, системы директорской и диспетчерской связи;

— устройства защиты абонентских однопрограммных громкоговорителей для блокирования утечки речевой ИсОД через радиотрансляционные линии;

— фильтры сетевые для блокирования утечки речевой ИсОД по цепям электропитания переменного (постоянного) тока;

— фильтры защиты линейные (высокочастотные) для установки в линиях аппаратов телеграфной (телекодовой) связи;

— генераторы линейного зашумления;

— генераторы пространственного зашумления;

— экранированные камеры специальной разработки.

Для телефонной связи, предназначенной для передачи ИсОД, рекомендуется применять аппараты отечественного производства, совместимые с устройствами защиты. Телефонные аппараты иностранного производства могут применяться при условии прохождения специсследований и положительного заключения компетентных организаций системы ТЗИ о их совместимости с устройствами защиты.

Выбор методов и способов защиты элементов ТСПИ и ВТСС, обладающих микрофонным эффектом, зависит от величины их входного сопротивления на частоте 1 кГц.

Элементы с входным сопротивлением менее 600 Ом (головки громкоговорителей, электродвигатели вентиляторов, трансформаторы и т.п.) рекомендуется отключать по двум проводам или устанавливать в разрыв цепей устройства защиты с высоким выходным сопротивлением для снижения до минимальной величины информативной составляющей тока.

Элементы с высоким входным сопротивлением (электрические звонки, телефонные капсюли, электромагнитные реле) рекомендуется не только отключать от цепей, но и замыкать на низкое сопротивление или закорачивать, чтобы уменьшить электрическое поле от данных элементов, обусловленное напряжением, наведенным при воздействии акустического поля. При этом следует учитывать, что выбранный способ защиты не должен нарушать работоспособность технического средства и ухудшать его технические параметры.

Высокочастотные автогенераторы, усилители (микрофонные, приема, передачи, громкого-ворящей связи) и другие устройства, содержащие активные элементы, рекомендуется отключать от линий электропитания в “дежурном режиме” или “режиме ожидания вызова”.

Защиту ИсОД от утечки по кабелям и проводам рекомендуется осуществлять путем:

— применения экранирующих конструкций;

— раздельной прокладки кабелей ОТС, ТСПИ и ВТСС.

При невозможности выполнения требований по разносу кабелей электропитания ОТС, ТСПИ и ВТСС электропитание последних следует осуществлять либо экранированными кабелями, либо от разделительных систем, либо через сетевые фильтры.

Не допускается образование петель и контуров кабельными линиями. Пересечение кабельных трасс разного назначения рекомендуется осуществлять под прямым углом друг к другу.

Электропитание ОТС должно быть стабилизировано по напряжению и току для нормальных условий функционирования ОТС и обеспечения норм защищенности.

В цепях выпрямительного устройства источника питания необходимо устанавливать фильтры нижних частот. Фильтры должны иметь фильтрацию по симметричным и несимметричным путям распространения.

Необходимо предусмотреть отключение электросети от источника питания ОТС при исчезновении напряжения в сети, при отклонении параметров электропитания от норм, заданных в ТУ, и при появлении неисправностей в цепях электропитания.

Все металлические конструкции ОТС (шкафы, пульты, корпуса распределительных устройств и металлические оболочки кабелей) должны быть заземлены.

Заземление ОТС следует осуществлять от общего контура заземления, размещенного в пределах контролируемой территории, с сопротивлением заземления по постоянному току в соответствии с требованиями стандартов.

Система заземления должна быть единой для всех элементов ОТС и строиться по радиальной схеме.

Образование петель и контуров в системе заземления не допускается.

Экраны кабельных линий ОТС, выходящих за пределы контролируемой территории, должны заземляться в кроссах от общего контура заземления в одной точке для исключения возможности образования петель по экрану и корпусам.

В каждом устройстве должно выполняться условие непрерывности экрана от входа до выхода. Экраны следует заземлять только с одной стороны. Экраны кабелей не должны использоваться в качестве второго провода сигнальной цепи или цепи питания.

Экраны кабелей не должны иметь электрического контакта с металлоконструкциями. Для монтажа следует применять экранированные кабели с изоляцией или одевать на экраны изоляционную трубку.

В длинных экранированных линиях (микрофонных, линейных, звукоусилительных) рекомендуется делить экран на участки для получения малых сопротивлений для высокочастотных токов и каждый участок заземлять только с одной стороны.

*3***. Обнаружение устройств съема информации**

В 1915 году немцы установили электрический барьер вдоль границы между Бельгией и Голландией. Быстро убедившись, что постоянное пропускание тока в заграждении такой длины обходится очень дорого, они начали включать ток время от времени. Многие шпионы и пленные, пытавшиеся наудачу пройти через барьер, были убиты током. В конце концов была изготовлена резиновая одежда, предохраняющая от поражения электрическим током. Одежда была черного цвета, и поэтому носившие ее практически были невидимы с наступлением темноты. Было лишь одно неудобство: несколько комплектов такой одежды было добыто германской полицией и впоследствии всех, кто в такой одежде оказывался по соседству с заграждением или у кого вовремя обыска находили сходную одежду, почти наверняка расстреливали. В дальнейшем союзники вынуждены были прибегнуть к промышленному шпионажу, чтобы выяснить, в какой момент ток выключался.

В наше время, несомненно, в подобном случае применили бы специальные индикаторы. Из детективной литературы хорошо известно, что преступник всегда оставляет следы. Так же и любое техническое устройство вносит какие-то изменения в окружающее пространство.

И если задача разведки состоит в том, чтобы сделать эти изменения как можно более незаметными, то задача тех кто занят поиском подобной техники, состоит в том, чтобы по едва уловимым следам изменения физических параметров пространства обнаружить и обезвредить технические устройства и системы ведения разведки. Задача технической контрразведки усложняется тем, что, как правило, неизвестно, какое конкретное техническое устройство контроля информации применено. Поэтому работа но поиску и обезвреживанию технических средств наблюдения дает обнадеживающий результат только в том случае, если она проводится комплексно, т.е. обследуют одновременно все возможные пути утечки информации.

Приведем достаточно условную классификацию устройств поиска технических средств разведки:

I. Устройства поиска активного тина, т.е. исследующие отклик на какое-либо воздействие:

> нелинейные локаторы — исследуют отклик на воздействие электромагнитным полем;

> рентгенметры — просвечивание с помощью рентгеновской аппаратуры;

> магнитно-резонансные локаторы, использующие явление ориентации молекул в магнитном поле;

> акустические корректоры.

II. Устройства поиска пассивного типа:

> металлоискатели;

> тепловизоры;

> устройства и системы поиска по электромагнитному излучению;

> устройства поиска по изменению параметров телефонной линии (напряжения, индуктивности, емкости, добротности);

> устройства поиска но изменению магнитного поля (детекторы записывающей аппаратуры).

В силу различных причин практическое применение нашли далеко не все из перечисленных технических средств Например, рентгеновская аппаратура очень дорога и громоздка и применяется исключительно специальными государственными организациями. То же, но в меньшей степени, относится к магнитно-резонансным локаторам. Тепловизоры, приборы, которые могут обнаруживать разницу температур, измеряемую сотыми долями градуса, могут регистрировать тепловую мощность порядка 1 мкВт. Эти, относительно дешевые приборы, в состав которых входит компьютер, могли бы стать очень эффективными и универсальными с точки зрения поиска технических средств коммерческой разведки, т.к. любое техническое средство при своей работе выделяет в окружающее пространство тепло. Скорее всего, появление на рынке подобных устройств является делом не далекого будущего.

Более подробно остановимся на устройствах, относительно широко представленных на отечественном рынке Прежде всего, это пассивные устройства поиска, основанные па исследовании электромагнитного излучения приемники, сканеры, шумомеры, детекторы излучения инфракрасного диапазона, анализаторы спектра, частотомеры, измерительные панорамные приемники, селективные микровольтметры и тп

**Средства защиты информации в АС**

В настоящее время на рынке представлено большое разнообразие средств защиты информации, которые условно можно разделить на несколько групп:

* средства, обеспечивающие разграничение доступа к информации в автоматизированных системах;
* средства, обеспечивающие защиту информации при передаче ее по каналам связи;
* средства, обеспечивающие защиту от утечки информации по различным физическим полям, возникающим при работе технических средств автоматизированных систем;
* средства, обеспечивающие защиту от воздействия программ-вирусов;
* материалы, обеспечивающие безопасность хранения, транспортировки носителей информации и защиту их от копирования.

Основное назначение средств защиты первой группы - разграничение доступа к локальным и сетевым информационным ресурсам автоматизированных систем. СЗИ этой группы обеспечивают:

* идентификацию и аутентификацию пользователей автоматизированных систем;
* разграничение доступа зарегистрированных пользователей к информационным ресурсам;
* регистрацию действий пользователей;
* защиту загрузки операционной системы с гибких магнитных дисков и CD-ROM;
* контроль целостности СЗИ и информационных ресурсов.

В качестве идентификаторов пользователей применяются, как правило, условные обозначения в виде набора символов. Для аутентификации пользователей применяются пароли.

Ввод значений идентификатора пользователя и его пароля осуществляется по запросу СЗИ с клавиатуры. Многие современные СЗИ используют и другие типы идентификаторов - магнитные карточки, радиочастотные бесконтактные карточки, смарт-карточки, электронные таблетки Touch Memory и другие. Отдельно стоит сказать об использовании в качестве идентификатора индивидуальных биологических параметров (отпечаток пальца, радужная оболочка глаза), присущих каждому человеку. Использование в качестве идентификаторов индивидуальных биологических параметров характеризуется, с одной стороны, высшим уровнем конфиденциальности, а с другой - очень высокой стоимостью таких систем.

Разграничение доступа зарегистрированных пользователей к информационным ресурсам осуществляется СЗИ в соответствии с установленными для пользователей полномочиями. Как правило, СЗИ обеспечивают разграничение доступа к гибким и жестким дискам, логическим дискам, директориям, файлам, портам и устройствам. Полномочия пользователей устанавливаются с помощью специальных настроек СЗИ. По отношению к информационным ресурсам средствами защиты могут устанавливаться такие полномочия, как разрешение чтения, записи, создания, запуска исполняемых файлов и другие.

Системы защиты информации предусматривают ведение специального журнала, в котором регистрируются определенные события, связанные с действиями пользователей, например запись (модификация) файла, запуск программы, вывод на печать и другие, а также попытки несанкционированного доступа к защищаемым ресурсам и их результат.

Особо стоит отметить наличие в СЗИ защиты загрузки операционной системы с гибких магнитных дисков и CD-ROM, которая обеспечивает защиту самих средств защиты от "взлома" с использованием специальных технологий. В различных СЗИ существуют программные и аппаратно-программные реализации этой защиты, однако практика показывает, что программная реализация не обеспечивает необходимой стойкости.

Контроль целостности средств защиты и защищаемых файлов заключается в подсчете и сравнении контрольных сумм файлов. При этом используются различной сложности алгоритмы подсчета контрольных сумм.

Несмотря на функциональную общность средств защиты информации данной группы, СЗИ различных производителей различаются:

* условиями функционирования (операционная среда, аппаратная платформа, автономные компьютеры и вычислительные сети);
* сложностью настройки и управления параметрами СЗИ;
* используемыми типами идентификаторов;
* перечнем событий, подлежащих регистрации;
* стоимостью средств защиты.

С развитием сетевых технологий появился новый тип СЗИ - межсетевые экраны (firewalls), которые обеспечивают решение таких задач, как защита подключений к внешним сетям, разграничение доступа между сегментами корпоративной сети, защита корпоративных потоков данных, передаваемых по открытым сетям.

Защита информации при передаче ее по каналам связи осуществляется средствами криптографической защиты (СКЗИ). Характерной особенностью этих средств является то, что они потенциально обеспечивают наивысшую защиту передаваемой информации от несанкционированного доступа к ней. Помимо этого, СКЗИ обеспечивают защиту информации от модификации (использование цифровой подписи и имитовставки).

Как правило, СКЗИ функционируют в автоматизированных системах как самостоятельное средство, однако в отдельных случаях СКЗИ может функционировать в составе средств разграничения доступа как функциональная подсистема для усиления защитных свойств последних.

Обеспечивая высокую степень защиты информации, в то же время применение СКЗИ влечет ряд неудобств:

* стойкость СКЗИ является потенциальной, т.е. гарантируется при соблюдении ряда дополнительных требований, реализация которых на практике осуществляется довольно сложно (создание и функционирование ключевой системы, распределение ключей, обеспечение сохранности ключей, необходимость в получении лицензии на право эксплуатации средств, планирование и организация мероприятий при компрометации ключевой системы);
* относительно высокая стоимость эксплуатация таких средств.

В целом, при определении необходимости использования средств криптографической защиты информации, необходимо учитывать то, что применение СКЗИ оправдано в случаях явного перехвата действительно конфиденциальной информации.

Целью статьи не является широкое обсуждение средств защиты от утечки информации по различным физическим полям, возникающим при работе технических средств автоматизированных систем, однако отметим, что для защиты информации от утечки по физическим полям используются следующие методы и средства защиты:

* электромагнитное экранирование устройств или помещений, в которых расположена вычислительная техника;
* активная радиотехническая маскировка с использованием широкополосных генераторов шумов, которые широко представлены на нашем рынке.

Радикальным способом защиты информации от утечки по физическим полям является электромагнитное экранирование технических устройств и помещений, однако это способ требует значительных капитальных затрат и практически не применяется.

И несколько слов о материалах, обеспечивающих безопасность хранения, транспортировки носителей информации и защиту их от копирования. В основном это специальные тонкопленочные материалы с изменяющейся цветовой гаммой или голографические метки, которые наносятся на документы и предметы (в том числе и на элементы компьютерной техники автоматизированных систем). Они позволяют:

* идентифицировать подлинность объекта;

контролировать несанкционированный доступ к ним.

6**.Составление плана ТЗИ на объекте.**

Предупреждение возможных угроз и противоправных действий может быть обеспечено самыми различными мерами и средствами, начиная от создания климата глубоко осознанного отношения сотрудников к проблеме безопасности и защиты информации до создания глубокой, эшелонированной системы защиты физическими, аппаратными, программными и криптографическими средствами.

Предупреждение угроз возможно и путем получения нформации о готовящихся противоправных актах, планируемых хищениях, подготовительных действиях и других элементах преступных деяний. Для этих целей необходима работа сотрудников службы безопасности с информаторами в интересах наблюдения и объективной оценки ситуации как внутри коллектива сотрудников, особенно главных участков ее фирмы, так и вне, среди конкурентов и преступных формирований.

В предупреждении угроз весьма существенную роль играет информационно-аналитическая деятельность службы безопасности на основе глубокого анализа криминогенной обстановки и деятельности конкурентов и злоумышленников.

Выявление имеет целью проведение мероприятий по сбору, накоплению и аналитической обработке сведений о возможной подготовке преступных действий со стороны криминальных структур или конкурентов на рынке производства и сбыта товаров и продукции. Особое внимание в этом виде деятельности должно отводиться изучению собственных сотрудников. Среди них могут быть и недовольные, и неопытные, и "внедренные".

Обнаружение угроз - это действия по определению конкретных угроз и их источников, приносящих тот или иной вид ущерба. К таким действиям можно отнести обнаружение фактов хищения или мошенничества, а также фактов разглашения конфиденциальной информации или случаев несанкционированного доступа к источникам коммерческих секретов. В числе мероприятий по обнаружению угроз значительную роль могут сыграть не только сотрудники СБ, но и сотрудники линейных подразделений и служб фирмы, а также технические средства наблюдения и обнаружения правонарушений.

Пресечение или локализация угроз - это действия, направленные на устранение действующей угрозы и конкретных преступных действий. Например, пресечение подслушивания конфиденциальных переговоров за счет акустического канала утечки информации по вентиляционным системам.

Ликвидация последствий имеет целью восстановление состояния, предшествовавшего наступлению угрозы. Например, возврат долгов со стороны заемщиков. Это может быть и задержание преступника с украденным имуществом, и восстановление разрушенного здания от подрыва и др.

Все эти способы имеют целью защитить информационные ресурсы от противоправных посягательств и обеспечить:

1. предотвращение разглашения и утечки конфиденциальной информации;
2. воспрещение несанкционированного доступа к источникам конфиденциальной информации; сохранение целостности, полноты и доступности информации;
3. соблюдение конфиденциальности информации;
4. обеспечение авторских прав.

Защита от разглашения сводится в общем плане к разработке перечня сведений, составляющих коммерческую тайну предприятия. Эти сведения должны быть доведены до каждого сотрудника, допущенного к ним, с обязательством этого сотрудника сохранять коммерческую тайну. Одним из важных мероприятий является система контроля за сохранностью коммерческих секретов.

Защита от утечки конфиденциальной информации сводится к выявлению, учету и контролю возможных каналов утечки в конкретных условиях и к проведению организационных, организационно-технических и технических мероприятий по их ликвидации.

Защита от несанкционированного доступа к конфиденциальной "формации обеспечивается путем выявления, анализа и контроля возможных способов несанкционированного доступа и проникновения к источникам конфиденциальной информации и реализацией организационных, организационно-технических и технических мероприятий по противодействию НСД.

На практике в определенной степени все мероприятия по использованию технических средств защиты информации подразделяются на три группы:

1. организационные (в части технических средств);
2. организационно-технические;
3. технические.

Организационные мероприятия - это мероприятия ограничительного характера, сводящиеся основном, к регламентации доступа и использования технических средств обработки информации. Они, как правило, проводятся силами самой организации путем использования простейших организационных мер.

В общем плане организационные мероприятия предусматривают проведение следующих действий:

1. определение границ охраняемой зоны (территории): Охраняемая зона – это и есть кабинет директора (в моём варианте). Сама комната описана в пункте **1.** данной работы;
2. определение технических средств, используемых для обработки конфиденциальной информации в пределах контролируемой территории: используются такие ТС как телефон, компьютер;
3. определение "опасных", с точки зрения возможности образования каналов утечки информации, технических средств и конструктивных особенностей зданий и сооружений: данный вопрос описан в пункте **2.**. Основными каналами утечки информации на данном объекте являются: телефонные линии связи, акустический канал, ПЭМИН, цепи заземления;
4. выявление возможных путей проникновения к источникам конфиденциальной информации со стороны злоумышленников: данный вопрос описан в пункте **3.**;
5. реализация мер по обнаружению, выявлению и контролю за обеспечением защиты информации всеми доступными средствами: данный вопрос описан в пункте **4.**.

Организационные мероприятия выражаются в тех или иных ограничительных мерах. Можно выделить такие ограничительные меры, как территориальные, пространственные и временные.

Территориальные ограничения сводятся к умелому расположению источников на местности или в зданиях и помещениях, исключающих подслушивание переговоров или перехват сигналов радиоэлектронных средств.

Пространственные ограничения выражаются в выборе направлений излучения тех или иных сигналов в сторону наименьшей возможности их перехвата злоумышленниками.

Временные ограничения проявляются в сокращении до минимума времени работы технических средств, использовании скрытых методов связи, шифровании и других мерах защиты.

Одной из важнейших задач организационной деятельности является определение состояния технической безопасности объекта, его помещений, подготовка и выполнение организационных мер, исключающих возможность неправомерного овладения конфиденциальной информацией, воспрещение ее разглашения, утечки и несанкционированного доступа к охраняемым секретам.

Организационно-технические мероприятия обеспечивают блокирование разглашения и утечки конфиденциальных сведений через технические средства обеспечения производственной и трудовой деятельности, а также противодействие техническим средствам промышленного шпионажа с помощью специальных технических средств, устанавливаемых на элементы конструкций зданий, помещений и технических средств, потенциально образующих каналы утечки информации. В этих целях возможно использование:

* технических средств пассивной защиты, например фильтров, ограничителей и тому подобных средств развязки акустических, электрических и электромагнитных систем защиты сетей телефонной связи, энергоснабжения, радио- и часофикации и др.;
* технических средств активной защиты: датчиков акустических шумов и электромагнитных помех.

Организационно-технические мероприятия по защите информации можно подразделить на пространственные, режимные и энергетические.

Пространственные меры выражаются в уменьшении ширины диаграммы направленности, ослаблении боковых и заднего лепестков диаграммы направленности излучения радиоэлектронных средств (РЭС).

Режимные меры сводятся к использованию скрытых методов передачи информации по средствам связи: шифрование, квазипеременные частоты передачи и др.

Энергетические - это снижение интенсивности излучения и работа РЭС на пониженных мощностях.

Технические мероприятия - это мероприятия, обеспечивающие приобретение, установку и использование в процессе производственной деятельности специальных, защищенных от побочных излучений (безопасных) технических средств или средств, ПЭМИН которых не превышают границу охраняемой территории.

Технические мероприятия по защите конфиденциальной информации можно подразделить на скрытие, подавление и дезинформацию.

Скрытие выражается в использовании радиомолчания и создании пассивных помех приемным средствам злоумышленников.

Подавление - это создание активных помех средствам злоумышленников.

Дезинформация - это организация ложной работы технических средств связи и обработки информации; изменение режимов использования частот и регламентов связи; показ ложных демаскирующих признаков деятельности и опознавания.

Защитные меры технического характера могут быть направлены на конкретное техническое устройство или конкретную аппаратуру и выражаются в таких мерах, как отключение аппаратуры на время ведения конфиденциальных переговоров или использование тех или иных защитных устройств типа ограничителей, буферных средств, фильтров и устройств зашумления.

**7.Обеспечение ИБ выделенного объекта.**

**Защита телефонных линий**

  Среди всего многообразия способов несанкционированного перехвата информации особое место занимает прослушивание телефонных переговоров, поскольку телефонная линия - самый первый, самый удобный и при этом самый незащищенный источник связи между абонентами в реальном масштабе времени.   
    На заре развития телефонной связи никто особо не задумывался о защите линий от прослушивания, и электрические сигналы распространялись по проводам в открытом виде. В наше время микроэлектронной революции прослушать телефонную линию стало простым и дешевым делом. Можно уверенно заявить о том, что если злоумышленник принял решение о "разработке" объекта, то первое, что он скорее всего сделает, это начнет контроль телефонных переговоров. Его можно осуществлять, не заходя в помещение, при минимальных затратах и минимальном риске. Нужно просто подключить к телефонной линии объекта специальное приемно - передающее или регистрирующее устройство.   
    С точки зрения безопасности телефонная связь имеет еще один недостаток: возможность перехвата речевой информации из помещений, по которым проходит телефонная линия и где подключен телефонный аппарат. Это осуществимо даже тогда, когда не ведутся телефонные переговоры (так называемый микрофонный эффект телефона и метод высокочастотного (ВЧ) навязывания). Для такого перехвата существует специальное оборудование, которое подключается к телефонной линии внутри контролируемого помещения или даже за его пределами.   
    Для защиты обычных городских телефонных каналов сегодняшний официальный рынок представляет пять разновидностей специальной техники:

* криптографические системы защиты (для краткости - скремблеры);
* анализаторы телефонных линий;
* односторонние маскираторы речи;
* средства пассивной защиты;
* постановщики активной заградительной помехи.

**Защита сети питания и заземления.**

Для фильтрации сигналов в цепях питания ТСПИ используются разделительные трансформаторы и помехоподавляющие фильтры.

##### Разделительные трансформаторы.

Такие трансформаторы должны обеспечивать развязку первичной и вторичной цепей по сигналам наводки. Это означает, что во вторичную цепь трансформатора не должны проникать наводки, появляющиеся в цепи первичной обмотки. Проникновение наводок во вторичную обмотку объясняется наличием нежелательных резистивных и емкостных цепей связи между обмотками.

Для уменьшения связи обмоток по сигналам наводок часто применяется внутренний экран, выполняемый в виде заземленной прокладки или фольги, укладываемой между первичной и вторичной обмотками. С помощью этого экрана наводка, действующая в первичной обмотке, замыкается на землю. Однако электростатическое поле вокруг экрана также может служить причиной проникновения наводок во вторичную цепь.

Разделительные трансформаторы используются с целью решения ряда задач, в том числе для:

* разделения по цепям питания источников и рецепторов наводки, если они подключаются к одним и тем же шинам переменного тока;
* устранения асимметричных наводок;
* ослабления симметричных наводок в цепи вторичной обмотки, обусловленных наличием асимметричных наводок в цепи первичной обмотки.

Средства развязки и экранирования, применяемые в разделительных трансформаторах, обеспечивают максимальное значение сопротивления между обмотками и создают для наводок путь с малым сопротивлением из первичной обмотки на землю. Это достигается обеспечением высокого сопротивления изоляции соответствующих элементов конструкции (~104 МОм) и незначительной емкости между обмотками. Указанные особенности трансформаторов для цепей питания обеспечивают более высокую степень подавления наводок, чем обычные трансформаторы [128].

Разделительный трансформатор со специальными средствами экранирования и развязки обеспечивает ослабление информационного сигнала наводки в нагрузке на 126 дБ при емкости между обмотками 0,005 пФ и на 140 дБ при емкости между обмотками 0,001 пФ.

Средства экранирования, применяемые в разделительных трансформаторах, должны не только устранять влияние асимметричных наводок на защищаемое устройство, но и не допустить на выходе трансформатора симметричных наводок, обусловленных асимметричными наводками на его входе. Применяя в разделительных трансформаторах специальные средства экранирования, можно существенно (более чем на 40 дБ) уменьшить уровень таких наводок.

##### Помехоподавляющие фильтры.

В настоящее время существует большое количество различных типов фильтров, обеспечивающих ослабление нежелательных сигналов в разных участках частотного диапазона. Это фильтры нижних и верхних частот, полосовые и заграждающие фильтры и т.д. Основное назначение фильтров - пропускать без значительного ослабления сигналы с частотами, лежащими в рабочей полосе частот, и подавлять (ослаблять) сигналы с частотами, лежащими за пределами этой полосы.

Для исключения просачивания информационных сигналов в цепи электропитания используются **фильтры нижних частот**.

Фильтр нижних частот **(ФНЧ)** пропускает сигналы с частотами ниже граничной частоты (f ≤ fгр) и подавляет- с частотами выше граничной частоты.

Последовательная ветвь ФНЧ должна иметь малое сопротивление для постоянного тока и нижних частот. Вместе с тем для того, чтобы высшие частоты задерживались фильтром, последовательное сопротивление должно расти с частотой. Этим требованиям удовлетворяет индуктивность L.

Параллельная ветвь ФНЧ, наоборот, должна иметь малую проводимость для низких частот с тем, чтобы токи этих частот не шунтировались параллельным плечом. Для высоких частот параллельная ветвь должна иметь большую проводимость, тогда колебания этих частот будут ею шунтироваться, и их ток на выходе фильтра будет ослабляться. Таким требованиям отвечает емкость С.

Более сложные многозвенные ФНЧ (Чебышева, Баттерворта, Бесселя и т.д.) конструируют на основе сочетаний различных единичных звеньев.

Количественно величина ослабления (фильтрации) нежелательных (в том числе и опасных) сигналов защитным фильтром оценивается в соответствии с выражением:

, дБ,



где U1 (P1) - напряжение (мощность) опасного сигнала на входе фильтра;

U2 (P2) - напряжение (мощность) опасного сигнала на выходе фильтра при включенной нагрузке ZH.

Основные требования, предъявляемые к защитным фильтрам, заключаются в следующем:

* величины рабочего напряжения и тока фильтра должны соответствовать напряжению и току фильтруемой цепи;
* величина ослабления нежелательных сигналов в диапазоне рабочих частот должна быть не менее требуемой;
* ослабление полезного сигнала в полосе прозрачности фильтра должно быть незначительным;
* габариты и масса фильтров должны быть минимальными;
* фильтры должны обеспечивать функционирование при определенных условиях эксплуатации (температура, влажность, давление) и механических нагрузках (удары, вибрация и т.д.);
* конструкции фильтров должны соответствовать требованиям техники безопасности.

К фильтрам цепей питания наряду с общими предъявляются следующие дополнительные требования:

* затухание, вносимое такими фильтрами в цепи постоянного тока или переменного тока основной частоты, должно быть минимальным (например, 0,2 дБ и менее) и иметь большое значение (более 60 дБ) в полосе подавления, которая в зависимости от конкретных условий может быть достаточно широкой (до 10 ГГц);
* сетевые фильтры должны эффективно работать при сильных проходящих токах, высоких напряжениях и высоких уровнях мощности проходящих и задерживаемых электромагнитных колебаний;
* ограничения, накладываемые на допустимые уровни нелинейных искажений формы напряжения питания при максимальной нагрузке, должны быть достаточно жесткими (например, уровни гармонических составляющих напряжения питания с частотами выше 10 кГц должны быть на 80 дБ ниже уровня основной гармоники).

**Рассмотрим влияние этих параметров более подробно.**

Напряжение, приложенное к фильтру, должно быть таким, чтобы оно не вызывало пробоя конденсаторов фильтра при различных скачках питающего напряжения, включая скачки, обусловленные переходными процессами в цепях питания. Чтобы при заданных массе и объеме фильтр обеспечивал наилучшее подавление наводок в требуемом диапазоне частот, его конденсаторы должны обладать максимальной емкостью на единицу объема или массы. Кроме того, номинальное значение рабочего напряжения конденсаторов выбирают исходя из максимальных значений допускаемых скачков напряжения цепи питания, но не более их.

**Ток** через фильтр должен быть таким, чтобы не возникало насыщения сердечников катушек фильтра. Кроме того, следует учитывать, что с увеличением тока через катушку увеличивается реактивное падение напряжения на ней. Это может привести к тому, что:

* ухудшается эквивалентный коэффициент стабилизации напряжения в цепи питания, содержащей фильтр;
* возникает взаимозависимость переходных процессов в различных нагрузках цепи питания.

Наибольшие скачки напряжения при этом возникают во время отключения нагрузок, так как большинство из них имеет индуктивный характер.

Характеристики фильтров зависят от числа использованных реактивных элементов. Так, например, фильтр из одного параллельного конденсатора или одной последовательной индуктивной катушки может обеспечить затухание лишь 20 дБ/декада вне полосы пропускания, a LC-фильтр из десяти или более элементов - более 200 дБ/декада.

Из-за паразитной связи между входом и выходом фильтра на практике трудно получить затухание более 100 дБ. Если фильтр неэкранированный и сигнал подается на него и снимается с помощью неэкранированных соединений (проводов), то развязка между входом и выходом обычно не превышает 40 ... 60 дБ. Для обеспечения развязки более 60 дБ необходимо использовать экранированные фильтры с разъемами и использовать для соединения экранированные провода.

Фильтры с гарантируемым затуханием 100 дБ выполняют в виде узла с электромагнитным экранированием, который помещается в корпус, изготовленный из материала с высокой магнитной проницаемостью магнитного экрана. Этим существенно уменьшается возможность возникновения внутри корпуса паразитной связи между входом и выходом фильтра из-за магнитных электрических или электромагнитных полей.

Из-за влияния паразитных емкостей и индуктивностей фильтр зачастую не обеспечивает требуемого затухания на частотах, превышающих граничную частоту (fС) на две декады, и полностью может потерять работоспособность на частотах, превышающих граничную частоту на несколько декад.

Ориентировочные значения максимального затухания для сетевых фильтров, приведены в табл.

**Таблица**

Значения максимального затухания для сетевых фильтров

|  |  |  |  |
| --- | --- | --- | --- |
| Диапазон частот | Максимальное затухание фильтра вне полосы пропускания, дБ | | |
| экранированный | | неэкранированный |
| с разъемами | без разъемов |
| Фильтры в цепях питания на токи не более 10 А | | | |
| fc≤ f ≤ 10 fc | 80 | — | — |
| 10fc≤ f ≤ 100 fc | 80 | — | — |
| f > 100 fc | 70 | — | — |
| Фильтры в цепях питания на токи более 1 0 А | | | |
| fc  ≤ f ≤ 10 fc; | 100 | — | — |
| 10fc ≤ f ≤ 100 fc | 100 | — | — |
| f > 100 fc | 90 | — | — |

Конструктивно фильтры подразделяются на:

* фильтры на элементах с сосредоточенными параметрами (LC-фильтры) - обычно предназначены для работы на частотах до 300 МГц;
* фильтры с распределенными параметрами (полосковые, коаксиальные или волноводные) - применяются на частотах свыше 1 ГГц;
* комбинированные - применяются на частотах 300 МГц ... 1 ГГц.

В настоящее время промышленностью выпускаются несколько серий защитных фильтров (ФП, ФБ, ФПС и др.). На рис. 4.8 ... 4.10 представлены принципиальные электрические схемы фильтров типа ФП, обеспечивающих эффективность фильтрации не менее 60 дБ, 80 дБ и 100 дБ соответственно.

Фильтры серии ФП обеспечивают затухание от 60 до 100 дБ. Они рассчитаны на номинальное напряжение переменного тока от 60 до 500 В и ток - от 2,5 до 70 А. Размеры фильтров составляют от 350•100•60 до 560•210•80 мм, а вес - от 2,5 до 25 кг.

Фильтры серии ФСПК-100 (200) предназначены для установки в четырехпроводных линиях электропитания частотой 50 Гц и напряжением 220/380 В. Максимальный рабочий ток составляет 100 (200) А. В диапазоне частот от 0,02 до 1000 МГц фильтры обеспечивают затухание сигнала не менее 60 дБ.

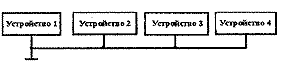
Конструктивно фильтры ФСПК выполнены в виде двух корпусов (полукомплектов), каждый из которых обеспечивает фильтрацию двухпроводной линии. Размеры одного корпуса составляют 800•320•92 мм, а вес- 18кг.

**Необходимо помнить**, что экранирование ТСПИ и соединительных линий эффективно только при правильном их заземлении. Поэтому одним из важнейших условий по защите ТСПИ является правильное заземление этих устройств.

В настоящее время существуют различные типы заземлений. Наиболее часто используются одноточечные, многоточечные и комбинированные (гибридные) схемы.

На рис. представлена одноточечная последовательная схема заземления.

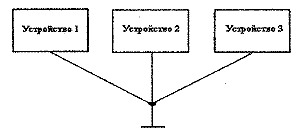
**Рис. Одноточечная последовательная схема заземления**



Эта схема наиболее проста. Однако ей присущ недостаток, связанный с протеканием обратных токов различных цепей по общему участку заземляющей цепи. Вследствие этого возможно появление опасного сигнала в посторонних цепях.

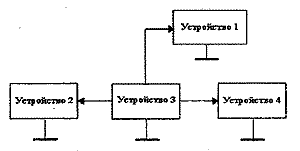
В одноточечной параллельной схеме заземления этого недостатка нет. Однако такая схема требует большого числа протяженных заземляющих проводников, из-за чего может возникнуть проблема с обеспечением малого сопротивления заземления участков цепи. Кроме того, между заземляющими проводниками могут возникать нежелательные связи, которые создают несколько путей заземления для каждого устройства. В результате в системе заземления могут возникнуть уравнительные токи и появиться разность потенциалов между различными устройствами.

**Рис. Одноточечная параллельная схема заземления**



Многоточечная схема заземления практически свободна от недостатков, присущих одноточечной схеме. В этом случае отдельные устройства и участки корпуса индивидуально заземлены. При проектировании и реализации многоточечной системы заземления необходимо принимать специальные меры для исключения замкнутых контуров.

**Рис. Многоточечная схема заземления**



Как правило, одноточечное заземление применяется на низких частотах при небольших размерах заземляемых устройств и расстояниях между ними менее 0,5•λ. На высоких частотах при больших размерах заземляемых устройств и значительных расстояниях между ними используется многоточечная система заземления. В промежуточных случаях эффективна комбинированная (гибридная) система заземления, представляющая собой различные сочетания одноточечной, многоточечной и плавающей заземляющих систем.

Заземление технических средств систем информатизации и связи должно быть выполнено в соответствии с определенными правилами.

Основные требования, предъявляемые к системе заземления, заключаются в следующем:

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

Довольно часто применяют заземляющее устройство в виде вертикально вбитой трубы. Сопротивление заземления в этом случае определяется формулой

, Ом,



где *l* - длина трубы, см;

rT - радиус трубы, см.

Из формулы видно, что сопротивление заземления зависит в большей степени не от радиуса трубы, а от ее длины. Поэтому при устройстве заземления целесообразнее применять тонкие и длинные трубы (стержни из арматуры).

При повышенных требованиях к величине сопротивления заземления (сопротивление заземления ТСПИ не должно превышать 4 Ом) применяют многократное заземление, состоящее из ряда одиночных симметрично расположенных заземлителей, соединенных между собой.

На практике наиболее часто в качестве заземлителей применяют:

* стержни из металла, обладающие высокой электропроводностью, погруженные в землю и соединенные с наземными металлоконструкциями средств ТСПИ;
* сеточные заземлители, изготовленные из элементов с высокой электропроводностью и погруженные в землю (служат в качестве дополнения к заземляющим стержням).

При необходимости устройства высокочастотного заземления нужно учитывать не только геометрические размеры заземлителей, их конструкцию и свойства почвы, но и длину волны высокочастотного излучения. Суммарное высокочастотное сопротивление заземления ZS складывается из высокочастотного сопротивления магистрали заземления ZM (провода, идущего от заземляемого устройства до поверхности земли) и из высокочастотного сопротивления самого заземлителя Z3 (провода, металлического стержня или листа, находящегося в земле).

Величина заземления в основном определяется не сопротивлением заземления, а сопротивлением заземляющей магистрали. Для уменьшения последнего следует стремиться прежде всего к уменьшению индуктивности заземляющей магистрали, что достигается за счет уменьшения ее длины и изготовления магистрали в виде ленты, обладающей по сравнению с проводом круглого сечения меньшей индуктивностью. В тех случаях, когда индуктивность заземляющей магистрали можно сделать весьма небольшой или использовать ее для получения последовательного резонанса при блокировании излучающих сетей защитными конденсаторами на землю (например, при комплексном подавлении излучения в помещениях), целесообразно значительно уменьшить величину сопротивления заземлителя Z3. Уменьшить величину Z3 можно также многократным заземлением из симметрично расположенных заземлителей.

При этом общее сопротивление заземления будет тем меньше, чем дальше друг от друга расположены отдельные заземлители.

При устройстве заземления в качестве заземлителей чаще всего применяются стальные трубы длиной 2 ... 3 м и диаметром 35 ... 50 мм и стальные полосы сечением 50 ... 100 мм.

Наиболее пригодными являются трубы, позволяющие достигнуть глубоких и наиболее влажных слоев земли, обладающих наибольшей проводимостью и не подвергающихся высыханию или промерзанию. Однако здесь необходимо учитывать, что с уменьшением сопротивления грунта возрастает коррозия металла. Кроме того, применение таких заземлителей не связано со значительными земляными работами, что неизбежно, например, при выполнении заземления из металлических листов или горизонтально закладываемых в землю металлических лент и проводов.

Заземлители следует соединять между собой шинами с помощью сварки. Сечение шин и магистралей заземления по условиям механической прочности и получения достаточной проводимости рекомендуется брать не менее (24 • 4) мм2.

Проводник, соединяющий заземлитель с контуром заземления, должен быть луженым для уменьшения гальванической коррозии, а соединения должны быть защищены от воздействия влаги.

Магистрали заземления вне здания необходимо прокладывать на глубине около 1,5 м, а внутри здания - по стене или специальным каналам таким образом, чтобы их можно было внешне осматривать. Соединяют магистрали с заземлителем только с помощью сварки. К заземляемому устройству ТСПИ магистраль подключают с помощью болтового соединения в одной точке.

Для уменьшения сопротивлений контактов наилучшим является постоянное непосредственное соединение металла с металлом, полученное сваркой или пайкой. При соединении под винт необходимо применять шайбы (звездочки или Гровера), обеспечивающие постоянство плотности соединения.

При соприкосновении двух металлов в присутствии влаги возникает гальваническая и (или) электрическая коррозия. Гальваническая коррозия является следствием образования гальванического элемента, в котором влага является электролитом. Степень коррозии определяется положением этих металлов в электрическом ряду.

Электрическая коррозия может возникнуть при соприкосновении в электролите двух одинаковых металлов. Она определяется наличием локальных электротоков в металле, например, токов в заземлениях силовых цепей.

Наиболее эффективным методом защиты от коррозии является применение металлов с малой электрохимической активностью, таких, как олово, свинец, медь. Значительно уменьшить коррозию и обеспечить хороший контакт можно, тщательно изолируя соединения от проникновения влаги.

**Защита от ПЭМИН**

Для защиты информации от утечки за счет ПЭМИН применяются пассивный, актив­ный и комбинированный методы. Пассивная защита заключается в сни­жении уровней излучения до величин, соизмеримых с естественными шу­мами, с помощью специальной элементной базы и конструктивной дора­ботки техники, обрабатывающей конфиденциальную информацию. Суще­ствуют различные способы реализации этого метода. Одно из самых про­стых технических решений состоит в том, чтобы поместить все оборудо­вание в безопасную и экранирующую радиоизлучения среду. Это приме­няется для малогабаритной аппаратуры, позволяя сохранять ее стоимость на приемлемом уровне. Для больших систем экранирование целых залов и даже зданий может быть чрезвычайно дорогим, поэтому проблемы обес­печения электронной защиты для них рассматриваются на стадии проек­тирования. Например, для систем связи определяются требования безо­пасности отдельных компонентов каждой секции всей системы. Разработ­чик может потребовать экранирования отдельных устройств системы при помощи металлического защитного покрытия или использовать стандарт­ные экранированные корпуса для блоков аппаратуры. Там, где экраниро­вание компонентов нецелесообразно, предусматривается достаточная изоляция линий данных и питания за счет различных сочетаний фильтров,

устройств подавления сигнала, низкоимпедансного заземления, транс­форматоров развязки. Должны также экранироваться кабели. При этом лучшим вариантом защиты линий связи является применение волоконно-оптической технологии. Надежное экранирование абонентской аппарату­ры связи чрезвычайно усложняет задачу электронного подслушивания.

Допустимые уровни излучений аппаратуры и меры защиты инфор­мации регламентируются специальными стандартами. В США, например, а также в ряде других западных стран в этих целях принят стандарт *"Tempest" (Transient Electromagnetic Pulse Ewanarions Standard).* Сущест­вуют полный и ослабленный варианты данного стандарта. В США по­следний введен в действие в 1990 году. Полный стандарт используется для защиты секретной информации министерства обороны и дипломати­ческой службы, а ослабленный для защиты "чувствительной" информации банков, фирм и других организаций.

В последние годы наблюдается устойчивый рост производства и продаж за рубежом оборудования, отвечающего требованиям стандарта *"Tempest".* Этому способствует все более широкое его применение на коммерческом рынке. Стоимость оборудования, отвечающего данному стандарту, как правило, в 3-5 раз выше стоимости соответствующего не­защищенного варианта.

Активная защита предполагает сокрытие информационных сигна­лов за счет шумовой или заградительной помехи с помощью специальных генераторов шума. Рассмотрим требования, предъявляемые к зашумляющим сигналам. При определении оптимальных пара­метров шума рассматривают две группы критериев — информационные и энергетические.

Сначала по информационным критериям обеспечи­вают самое высокое качество помехового сигнала, за­тем выбирают его параметры, при которых обеспечи­вается зашумление информации при наименьшей мощности шума.

Идеальные маскирующие помеховые сигналы дол­жны создавать такие условия, при которых апостери­орная вероятность опознавания была бы равна нулю при максимальной априорной вероятности наличия сигнала с известными параметрами. Это исключает возможность применения для цепей маскировки детер­минированных помеховых сигналов, так как они лег­ко распознаются, а поэтому не могут увеличить нео­пределенность в системе.

Поскольку детерминированные помеховые сигна­лы обладают низкими потенциальными возможностя­ми маскировки, их можно устранить сравнительно простыми техническими приемами. Маскирующие по­меховые сигналы должны содержать элемент неопре­деленности.

Мерой неопределенности случайных величин или случайного процесса является энтропия. При прочих равных условиях среды маскирующих помеховых сиг­налов (шумов) лучшим является тот, энтропия которо­го больше. Шум, создаваемый реальными источника­ми, имеет ограничения как по максимально достижимым значениям, так и по средней мощности (дисперсии). Следовательно, из всех ограниченных сверху и снизу шумов, представленных одномерным распределением, максимальную энтропию имеет тот, у которого плотность распределения вероятности явля­ется равномерной.

В реальных условиях шумовое напряжение ограни­чено как по средней мощности, так и по максималь­ным вопросам, в результате чего оптимальное распре­деление будет отличаться от равномерного и от гауссова. Чтобы обеспечить маскирование при наи­меньшей мощности шума, параметры маскирующего шума выбирают с учетом параметра защищаемых сиг­налов. Сигналы, циркулирующие в технических сред­ствах, имеют ограниченный спектр, поэтому для их зашумления энергетически целесообразно выбирать зашумляющие сигналы, лежащие в той же области ча­стот.

Следует также учитывать, что статистические пара­метры информационного сигнала известны злоумыш­леннику и он может применять приемные устройства с оптимальным фильтром. Исходя из этого необходи­мо, чтобы шум также прошел оптимальную обработку. Самым сильным маскирующим эффектом при наи­меньшей мощности шумового генератора будет обла­дать шум со спектром, повторяющим спектр зашумляемого сигнала.

Еще больший выигрыш обеспечивается при зашумлении телевизионных сигналов шумом, прошедшим оптимальную обработку. Основная доля энергии видео­сигнала заключена в строчной структуре, поэтому оп­тимальным устройством для обнаружения видеосигна­ла в шумах будет устройство, имеющее передаточную характеристику, определяемую спектром последова­тельности строчных гасящих импульсов. Применение для активной защиты помехового сигнала, имеющего нормальный закон распределения в видимой части строки и распределение спектральной плотности, по­добное строчной структуре защищаемого видеосигна­ла обеспечивает выигрыш в энергии более чем в 20 раз по сравнению с применением для этой цели квазибе­лого шума.

С учетом рассмотренных требований к шуму струк­турная схема устройства зашумления должна состоять из последовательно соединенных генераторов шума, узла формирования шума с требуемой спектральной харак­теристикой, усилителя и узла сопряжения с нагрузкой.

Активная радиотехническая маскировка заключается в формировании и излучении маскирующего сигнала в непосредственной близости от маскируемой системы. В данном случае различают энергети­ческий и неэнергетический методы активной радиотехнической маски­ровки.

При энергетической маскировке получается широкополосный шу­мовой сигнал с уровнем, существенно превышающим во всем частотном диапазоне уровень излучения системы. Одновременно происходит навод­ка шумовых колебаний в отходящих цепях. Энергетическая маскировка может быть реализована только в случае, если уровень излучений сущест­венно меньше установленного существующими стандартами на электро­магнитную совместимость и медицинскими требованиями. В противном случае устройство маскировки или будет создавать помехи различным радиоустройствам, расположенным поблизости от защищаемой системы, или его нельзя будет использовать по медицинским соображениям.

Неэнергетический метод активной радиотехнической маскировки (статистический) заключается в изменении вероятностной структуры сиг­нала, который может быть принят приемником злоумышленника. Для такого изменения сигнала необходимо специальное устройство, которое может встраиваться непосредственно в систему или размещаться рядом. Уровень излучаемого этим устройством маскирующего сигнала не превос­ходит уровня информативного излучения системы, поэтому подобные уст­ройства не создают ощутимых помех для других электронных приборов, находящихся рядом, а также безопасны для здоровья оператора системы.

Комбинированная защита - это снижение уровней излучения до за­данных значений с одновременным использованием и пассивной, и ак­тивной защиты.

Защита от НСВ

Для обеспечения защиты АС от НСВ по коммуникационным каналам (главным образом речь идет о проводных линиях связи) необходимо проведение определенных мероприятий организационного и технического характера. Их детализация требует привязки к конкретному объекту.

1. Необходимо проверить с привлечением квалифицированных специалистов схему внутренних и внешних коммуникационных каналов объекта для выявления возможных путей для нападения на объект по проводным линиям связи.
2. Схема внутренних и внешних коммуникационных каналов объекта должна быть разделена на зоны, в которых можно реализовать те или иные мероприятия по защите.
3. На все проводные линии связи, которые выходят за пределы зон, подконтрольных службе безопасности объекта, должны быть установлены устройства защиты от НСВ для каждого проводника линий связи. Места для установки шкафов с защитным оборудованием выбираются в зонах, подконтрольных службе безопасности.
4. После завершения монтажа кабельных коммуникаций и УС снимается “портрет” коммуникационной сети с помощью анализатора неоднородностей линии связи. При последующем систематическом контроле коммуникационной сети, сравнивая результаты текущих измерений с контрольным “портретом” сети, можно будет выявить несанкционированные подключения. Таким способом весьма точно выявляются контактные подключения с емкостной развязкой, поскольку они имеют импеданс, существенно отличающийся от волнового сопротивления линий связи. Так как емкость разделительного конденсатора невелика, то зондирующий импульс должен иметь наносекундный диапазон.
5. Доступ к мини-АТС, кросс-панелям и другим элементам коммуникационных каналов связи должен быть ограничен соответствующими документами и техническими мероприятиями, а текущее обслуживание оборудования и ремонтные работы необходимо производить под контролем сотрудников режимной службы.
6. При проектировании схем размещения и монтаже коммуникационного оборудования АС необходимо устранять потенциальные возможности для атаки на объект с помощью ТС НСВ.

Общепринятая топология прокладки проводных линий связи, когда пары линий выполнены из плоского кабеля (“лапши”) и отдельные пары прокладываются вдоль поверхности стены параллельно одна другой, является идеальной для атаки на объект с помощью ТС НСВ с бесконтактным емкостным инжектором. С помощью плоского накладного электрода на изолирующей штанге и ТС с большой частотой следования пачек импульсов подключенные к таким линиям УС могут быть выведены из строя за 10–30 с. Поэтому подобная топология прокладки проводных линий связи допустима только в пределах контролируемой зоны.

Размещение АТС, кроссовых устройств, маршрутизаторов и других подобных устройств на внешних стенах объекта нежелательно, так как может быть произведена атака на объект с наружной стороны стены.

При атаке в зоне расположения АС или кабельных коммуникаций снаружи объекта накладывается емкостной бесконтактный инжектор большого размера (так как ограничений по скрытности атаки практически нет) и производится НСВ. Эффективность такого НСВ наиболее высока для помещений с тонкими стенами из современных искусственных материалов с большой диэлектрической проницаемостью, а минимальна для экранированных помещений и помещений с железобетонными стенами. В последнем случае эффективность НСВ снижается из-за экранирующего влияния арматуры железобетона. Поэтому, если возможности для замены тонкостенных перегородок нет, необходимо предусмотреть экранирование помещения при его проектировании (по меньшей мере, проводящими обоями или металлической сеткой). В особенности эта рекомендация актуальна для помещений с коммуникационным оборудованием, имеющих смежные комнаты вне зоны контроля. При невозможности экранирования всего помещения необходимо прокладывать линии связи по широкой заземленной полосе металла.

1. При закупках коммуникационного оборудования для АС необходимо обращать внимание на степень его защиты от импульсных помех. Наиболее важными являются следующие характеристики: степень защиты от микросекундных импульсных помех большой энергии (применительно к ТС НСВ с контактным подключением к низковольтным емкостным накопителям) и степень защиты от пачек импульсов наносекундного диапазона (применительно к ТС НСВ с высоковольтными трансформаторами и бесконтактными инжекторами).

Целесообразно ориентироваться на определенную минимальную степень защищенности оборудования АС по коммуникационным каналам, которая должна соответствовать ГОСТ.

1. При построении схемы защиты объекта целесообразно выделить три рубежа:

* рубеж I — защита по периметру объекта всех коммуникационных каналов для предотвращения внешней угрозы нападения с использованием ТС НСВ.
* рубеж II — поэтапная защита для локализации ТС НСВ, стационарно установленных внутри охраняемого объекта или пронесенных внутрь его для организации однократной атаки;

рубеж III — индивидуальная защита наиболее ответственных элементов АС.

Основными принципами защиты от НСВ по цепям питания являются следующие.

1. С привлечением квалифицированных специалистов-электриков необходимо проанализировать схему электроснабжения объекта для выявления возможных каналов для нападения на объект по цепям питания.
2. Схема электроснабжения объекта должна быть разделена на зоны, в которых можно организовать те или иные мероприятия по защите.
3. На все фидеры, которые выходят за пределы зон, должны быть установлены групповые устройства защиты от НСВ. Места для их установки выбираются в зонах защиты информации. Индивидуальная защита должна быть установлена, по меньшей мере, на сеть питания серверов, систем охраны и управления объекта.
4. При монтаже на объекте выделенной сети питания для АС необходимо розетки, щитки питания и прочее оборудование размещать в помещениях с оборудованием АС и в помещениях, находящихся под контролем. Не рекомендуется установка розеток и других устройств выделенной сети, к которым могут быть подключены ТС НСВ, в помещениях для отдыха, раздевалках, складах, буфетах и других слабо контролируемых помещениях. Соответствующими документами должно быть запрещено использование розеток выделенной сети питания для подключения пылесосов и другой бытовой техники, поскольку в такую технику могут встраиваться ТС НСВ.
5. После завершения монтажа электроснабжения снимается своеобразный “портрет” сети с помощью анализатора неоднородности линии. При последующем систематическом контроле сети электроснабжения с помощью анализатора и сравнения результатов текущих измерений с “портретом” сети можно будет выявить несанкционированное подключение. Таким способом весьма точно выявляются ТС НСВ последовательного типа, поскольку они имеют импеданс, существенно отличающийся от волнового сопротивления кабелей.
6. Доступ к щитам питания и другим элементам электрооборудования здания должен быть ограничен соответствующими документами и инструкциями, а также техническими мероприятиями. Текущее обслуживание электрооборудования и ремонтные работы должны проводиться под контролем сотрудников режимной службы. Заметим, что включение последовательных ТС НСВ в разрыв кабеля при доступе к щиту питания легко камуфлируется. Например, кабель от ТС НСВ подключается к клеммам предохранителя в щите питания. Предохранитель вынимается, при этом ТС НСВ оказывается включенным, а электропитание при включении не прерывается, после этого контакты предохранителя изолируются, и он для маскировки устанавливается на свое штатное место. После совершения нападения все восстанавливается в обратном порядке.
7. Все электрооборудование (в том числе и бытового назначения) должно тщательно проверяться. Чаще всего для маскировки ТС НСВ используются пылесосы, кондиционеры, микроволновые печи (в последних уже содержатся высоковольтные конденсаторы, зарядное устройство и другие узлы, позволяющие использовать их в качестве элементов ТС НСВ). Внимание режимных служб должны привлекать оставленные строителями или ремонтниками сварочные трансформаторы и подобное оборудование, особенно если все это оставлено подключенным к сети питания.
8. Желательно организовать на объекте круглосуточный мониторинг сети электропитания с помощью соответствующих регистрирующих приборов и одновременную регистрацию в журнале всех сбоев и повреждений оборудования с обязательной фиксацией времени возникновения сбоев и характера дефектов. Время возникновения сбоев и дефектов накладывается на распечатку параметров напряжения питающей сети. При выявлении скачков напряжения можно своевременно установить факт НСВ по сети питания, в том числе и с помощью ТС с параллельным подключением, которые не выявляются импульсным зондированием сети электропитания. Спектр регистрирующих приборов простирается от простого счетчика импульсов до сложных комплексов на базе ПЭВМ.
9. ТС НСВ с емкостным накопителем имеют демаскирующие акустические признаки — при разрядке конденсаторы генерируют акустический импульс. Это обстоятельство можно использовать для поиска ТС НСВ такого типа. Для простейших ТС, работающих периодично, это возможно, а для ТС со случайным законом генерирования импульсов поиск по акустическим шумам затруднен.
10. При закупках оборудования АС необходимо обращать внимание на степень его защиты от импульсных помех. Необходимо, чтобы оборудование имело класс устойчивости к импульсным перенапряжениям не ниже A по ITTT Standard 587-1980 и аналогичным западным стандартам (помеха — 0,5 мкс, 100 кГц, 6 кВ, 200 А, 1,6 Дж), для наиболее важного оборудования — класс B (помехи 0,5 мкс — 100 кГц, 6 кВ, 500 А, 4 Дж; 1,2/50 мкс — 6 кВ; 8/20 мкс — 3 кА, 80 Дж). Оборудование, подключаемое к витым парам в сети большой протяженности, должно также иметь надлежащую защиту по информационным каналам. Наибольшего внимания заслуживают модемы, работающие на внешние проводные или кабельные линии связи. Следует обращать особое внимание на способность модемов противостоять мощным импульсным помехам. Более половины моделей модемов в варианте поставки “для России” не имеют схем защиты телефонных линий, хотя вся необходимая для установки защитных устройств разводка на печатных платах присутствует. Поэтому не только при НСВ, но и при обычной эксплуатации такие модемы быстро выходят из строя. Более детальное рассмотрение вопросов защиты от НСВ по коммуникационным каналам приведено в следующем подразделе.

**Защита по виброакустическому каналу утечки информации**

Метод съема информации по виброакустическому каналу относится к так называемым беззаходовым методам, и это является важным его преимуществом. Обнаружить аппаратуру такого съема информации крайне трудно, так как она устанавливается за пределами контролируемого помещения, а в ряде случаев существенно удалена от него.

Кратко о физическом принципе, который лежит в основе этого метода. Речь, вызывающая акустические сигналы, представляет собой механические колебания воздушной среды. Попадая на твердые поверхности(стены, перегородки), они преобразуются в структурные вибрационные сигналы, которые, оставаясь по своей природе механическими, распространяется по строительным конструкциям здания. Можно выделить следующие типовые конструкции, по которым передаются речевые сигналы:

* В акустическом сигнале это- несущие стены зданий, перегородки, перекрытия зданий, окна, двери, вентиляционные воздуховоды;
* В вибрационном канале это- стены и перегородки, перекрытия, оконные рамы, дверные коробки, трубопроводы, короба вентиляции.

Если акустические датчики установлены на этих конструкциях за пределами помещения, это дает возможность принять речевые сигналы и проконтролировать разговоры внутри него. При этом необязательно скрытно проникать в помещение- достаточно приблизится к нему снаружи. Установить датчик можно и дистанционным способом- с помощью специальных выстреливающих устройств. Иногда используют лазерные устройства и направленные микрофоны. Действие лазерных устройств основано на принципе снятия вибрации(речевых сигналов) с оконного стекла, а направленные микрофоны снимают речевую информацию по акустическому каналу.

Для обратного преобразования механических колебаний в акустический сигнал служат контактные микрофоны, известные под названием стетоскопы. Электронные стетоскопы сначала преобразуют механические колебания в электрический сигнал, который затем усиливается и уже тогда преобразуется в акустический.

Итак, вибрационным каналом утечки информации здесь уже является не воздух, а другая среда распространения акустического сигнала. Такие каналы возникают при падении первичной акустической волны в воздухе на другую среду и дальнейшем распространении ее в новой среде. На практике - это стены, пол, потолок, двери и косяки, стекла, оконные рамы и коробки, инженерные коммуникации проходящие или выходящие из помещения.

Предотвращение утечки информации по этим каналам сводится, как и в случае с акустическими каналами, к двум направлениям:

1. Максимально ослабить акустический сигнал от источника звука, попадающий в другую среду распространения, где его могут перехватить. Заставить акустическую волну пройти сначала среду с высоким затуханием, например. Это означает, что отделка стен звукопоглощающими материалами предпочтительнее, чем простая оклейка обоями. Тяжелые портьеры на окнах значительно ослабляют акустический сигнал, попадающий на стекла. Красивые дубовые сплошные одинарные двери явно проигрывают по этому параметру двойным, обитым дерматином.

2. Создать в "опасной" среде распространения сильный помеховый сигнал, который невозможно отфильтровать от полезного. Само собой разумеется, что помехи и так есть - бульканье воды в трубах отопления, сверление бетонных стен соседями по дому, шум от проезжающих по улице тяжелых грузовиков и трамваев. Для зашумления используют уже упоминавшиеся генераторы белого шума, к которым подсоединяют специальные излучатели, устанавливаемые на стенах, стеклах, рамах, косяках, трубах отопления и т.д.

Из всего вышесказанного можно сделать следующие выводы:

* В общем случае акустический сигнал распространяется в упругих средах с затуханием, зависящем от свойств среды распространения.
* При переходе из одной среды в другую часть сигнала теряется ( отражение, поглощение).
* Виброакустическими каналами утечки информации является совокупность сред распространения сигнала от источника до приемника.

Анализ возможных каналов утечки информации, в нашем случае по виброакустическому каналу, требует методичного, кропотливого подхода. Не спешите, попробуйте с учетом всего вышесказанного посмотреть на эту проблему другими глазами. Начните с наиболее простого - акустического канала. Допустим, кабинет Вашего шефа расположен на втором этаже, окна выходят в тихий скверик. В жаркую погоду окна в течение рабочего дня открыты. Значит канал утечки есть. Можно ли им воспользоваться? Да, в 20 метрах от окна под деревом стоит скамейка. Расположившись на ней с закамуфлированным направленным микрофоном, злоумышленник, в принципе, может подслушать разговор в кабинете. Нужно защищать этот канал? Несомненно. Окна необходимо закрыть, в помещении установить кондиционер. Есть ли в помещении вентиляционные решетки? Да, есть. Выясняем, куда ведет уходит вентиляционный канал. Обычно на верхние этажи. Кто у нас сосед сверху? Трудно сказать, фирма какая-то арендует помещение. Вот и еще один возможный канал утечки информации. Необходимо применить защиту - устанавливаем в вентиляционное отверстие акустический излучатель генератора белого шума. И так далее, стараясь ничего не пропустить, но и реально оценивая возможности потенциального противника по использованию канала утечки информации. Очень полезно свои соображения по поводу обнаруженных каналов утечки и способов защиты изложить на бумаге. Это значительно облегчает как анализ угроз перехвата информации, так и выбор соответствующей аппаратуры защиты, в частности, в плане выбора ее технических параметров, количества приборов и определения общей стоимости защитных мероприятий.

В заключение несколько слов о выборе виброакустических генераторов шума. Прибор должен быть укомплектован излучателями, крепящимися на стенах, на инженерных коммуникациях, стеклах, а также акустическими колонками. Обратите внимание на способ крепления излучателей - сможете ли Вы обеспечить требования изготовителя по установке. Каждый излучатель, особенно устанавливаемые на стенах, "закрывает" определенную площадь. Подсчитайте, сколько излучателей Вам потребуется и проверьте способен ли генератор обеспечить нормальную работу всех подключаемых излучателей (большую роль здесь играет выходная мощность генератора). Одна из новейших разработок - "Прибор виброакустической защиты SI-3001".

В отличие от других генераторов он имеет два независимых канала, что позволяет дифференцированно подходить к конфигурированию ветвей виброакустической защиты. Повышенная выходная мощность каждого канала обеспечивает нормальную работу значительно большего, чем у других моделей, числа излучателей. При этом изделие работает со всеми типами излучателей, имеющимися на рынке. Это очень удобно, если Вы наращиваете или модернизируете свою систему защиты. Еще одной отличительной чертой является генерация наряду с обычным белым шумом речеподобной помехи, что значительно повышает степень защиты информации. Кроме того, использование речеподобной помехи позволяет снизить уровень шумовой помехи, подводимой к излучателю, что приводит к уменьшению паразитного шума в помещении. Особенностью прибора является также формирование шумовой помехи с автоматически регулируемым уровнем, чем громче Вы говорите, т.е. чем больше опасность перехвата, тем больше уровень шумового сигнала и наоборот.

**Звукоизоляция помещений** направлена на локализацию источников акустических сигналов внутри них и проводится с целью исключения перехвата акустической (речевой) информации по прямому акустическому (через щели, окна, двери, технологические проемы, вентиляционные каналы и т.д.) и вибрационному (через ограждающие конструкции, трубы водо-, тепло- и газоснабжения, канализации и т.д.) каналам.

Основное требование к звукоизоляции помещений заключается в том, чтобы за его пределами отношение акустический сигнал/шум не превышало некоторого допустимого значения, исключающего выделение речевого сигнала на фоне естественных шумов средством разведки. Поэтому к помещениям, в которых проводятся закрытые мероприятия, предъявляются определенные требования по звукоизоляции.

Учитывая, что средняя громкость звука говорящего в служебном помещении составляет около 50 ... 60 дБ, то в зависимости от категории помещения его звукоизоляция должна быть не менее норм, приведенных в табл. 4.1.

**Таблица 4.1**

Требования к звукоизоляции помещений

|  |  |  |  |
| --- | --- | --- | --- |
| **Частота, Гц** | **Категория выделенного помещения, дБ** | | |
| **1** | **2** | **3** |
| 500 | 53 | 48 | 43 |
| 1000 | 56 | 51 | 46 |
| 2000 | 56 | 51 | 46 |
| 4000 | 55 | 50 | 45 |

Звукоизоляция помещений обеспечивается с помощью архитектурных и инженерных решений, а также применением специальных строительных и отделочных материалов.

При падении акустической волны на границу поверхностей с различными удельными плотностями большая часть падающей волны отражается. Меньшая часть волны проникает в материал звукоизолирующей конструкции и распространяется в нем, теряя свою энергию в зависимости от длины пути и его акустических свойств. Под действием акустической волны звукоизолирующая поверхность совершает сложные колебания, также поглощающие энергию падающей волны.

Характер этого поглощения определяется соотношением частот падающей акустической волны и спектральных характеристик поверхности средства звукоизоляции.

Одним из наиболее слабых звукоизолирующих элементов ограждающих конструкций выделенных помещений являются двери и окна.

Двери имеют существенно меньшие по сравнению со стенами и межэтажными перекрытиями поверхностные плотности и трудноуплотняемые зазоры и щели. Стандартные двери не удовлетворяют требованиям по защите информации (см. табл. 4.2).

**Таблица 4.2**

Звукоизоляция обычных дверей

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Конструкция двери** | **Условия применения** | **Звукоизоляция (дБ) на частотах, Гц** | | | | | |
| **125** | **250** | **500** | **1000** | **2000** | **4000** |
| Щитовая дверь, облицованная фанерой с двух сторон | без прокладки | 21 | 23 | 24 | 24 | 24 | 23 |
| с прокладкой из пористой резины | 27 | 27 | 32 | 35 | 34 | 35 |
| Типовая дверь П-327 | без прокладки | 13 | 23 | 31 | 33 | 34 | 36 |
| с прокладкой из пористой резины | 29 | 30 | 31 | 33 | 34 | 41 |

Увеличение звукоизолирующей способности дверей достигается плотной пригонкой полотна двери к коробке, устранением щелей между дверью и полом, применением уплотняющих прокладок, обивкой или облицовкой полотен дверей специальными материалами и т.д.

Как видно из табл. 4.2, применение уплотняющих прокладок повышает звукоизоляцию дверей, однако при этом необходимо учитывать, что в процессе эксплуатации в результате обжатия, износа, затвердевая резиновых прокладок звукоизоляция существенно снижается.

**Таблица 4.4**

Звукоизоляция окон

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Схема остекления** | **Звукоизоляция (дБ) на частотах, Гц** | | | | | |
| **125** | **250** | **500** | **1000** | **2000** | **4000** |
| **Одинарное остекление:** |  | | | | | |
| толщина 3 мм | 17 | 17 | 22 | 28 | 31 | 32 |
| толщина 4 мм | 18 | 23 | 26 | 31 | 32 | 32 |
| толщина 6 мм | 22 | 22 | 26 | 30 | 27 | 25 |
| **Двойное остекление с воздушным промежутком:** |  | | | | | |
| 57 мм (толщина 3 мм) | 15 | 20 | 32 | 41 | 49 | 46 |
| 90 мм (толщина 3мм) | 21 | 29 | 38 | 44 | 50 | 48 |
| 57 мм (толщина 4 мм) | 21 | 31 | 38 | 46 | 49 | 35 |
| 90 мм (толщина 4 мм) | 25 | 33 | 41 | 47 | 48 | 36 |

Для повышения звукоизоляции проводится облицовка внутренних поверхностей тамбура звукопоглощающими покрытиями, а двери обиваются материалами со слоями ваты или войлока и используются дополнительные уплотнительные прокладки.

Звукопоглощающая способность окон, так же как и дверей, зависит, главным образом, от поверхностной плотности стекла и степени прижатия притворов. В табл. 4.4 указаны некоторые данные по звукоизоляции наиболее распространенных вариантов остекления помещений.

Звукоизоляция окон с одинарным остеклением соизмерима со звукоизоляцией одинарных дверей и недостаточна для надежной защиты информации в помещении. Существенно большую звукоизоляцию имеют окна с остеклением в раздельных переплетах с шириной воздушного промежутка более 200 мм или тройное комбинированное остекление.

Обычные окна с двойными переплетами обладают более высокой (на 4 ... 5 дБ) звукоизолирующей способностью по сравнению с окнами со спаренными переплетами. Применение упругих прокладок значительно улучшает звукоизоляционные качества окон. В случаях, когда необходимо обеспечить повышенную звукоизоляцию, применяют окна специальной конструкции (например, двойное окно с заполнением оконного проема органическим стеклом толщиной 20 ... 40 мм и с воздушным зазором между стеклами не менее 100 мм). Разработаны конструкции окон с повышенным звукопоглощением на основе стеклопакетов с герметизацией воздушного промежутка между стеклами и с заполнением его различными газовыми смесями или создание в нем вакуума. Повышение звукоизоляции до 5 дБ наблюдается при облицовке межстекольного пространства по периметру звукопоглощающим покрытием.

Необходимо отметить, что увеличение числа стекол не всегда приводит к увеличению звукоизоляции в диапазоне частот речевого сигнала вследствие резонансных явлений в воздушных промежутках и эффекта волнового совпадения.

Для повышения звукоизоляции в помещениях применяют акустические экраны, устанавливаемые на пути распространения звука на наиболее опасных (с точки зрения разведки) направлениях.

Действие акустических экранов основано на отражении звуковых волн и образовании за экраном звуковых теней. С учетом дифракции эффективность экрана повышается с увеличением соотношения размеров экрана и длины акустической волны. Размеры эффективных экранов превышают более чем в 2-3 раза длину волны. Реально достигаемая эффективность акустического экранирования составляет 8... 10дБ.

Применение акустического экранирования целесообразно при временном использовании помещения для защиты акустической информации. Наиболее часто применяются складные акустические экраны, используемые для дополнительной звукоизоляции дверей, окон, технологических проемов, систем кондиционирования, проточной вентиляции и других элементов ограждающих конструкций, имеющих звукоизоляцию, не удовлетворяющую действующим нормам.

Для повышения звукоизоляции помещений также применяют звукопоглощающие материалы.

Звукопоглощение обеспечивается путем преобразования кинетической энергии акустической волны в тепловую энергию в звукопоглощающем материале. Звукопоглощающие свойства материалов оцениваются коэффициентом звукопоглощения, определяемым отношением энергии звуковых волн, поглощенной в материале, к падающей на поверхность материала и проникающей (неотраженной) в звукопоглощающий материал.

Применение звукопоглощающих материалов при защите акустической информации имеет некоторые особенности по сравнению с звукоизоляцией. Одной из особенностей является необходимость создания непосредственно в помещении акустических условий для обеспечения разборчивости речи в различных его зонах. Таким условием является прежде всего обеспечение оптимального соотношения прямого и отраженного от ограждений акустических сигналов. Чрезмерное звукопоглощение приводит к ухудшению уровня сигнала в различных точках помещения, а большое время реверберации - к ухудшению разборчивости в результате наложения различных звуков.

Обеспечение рациональных значений рассмотренных условий определяется как общим количеством звукопоглощающих материалов в помещении, так и распределением звукопоглощающих материалов по ограждающим конструкциям с учетом конфигурации и геометрических размеров помещений.

Звукопоглощающие материалы могут быть сплошными и пористыми. Обычно пористые материалы используют в сочетании со сплошными.

Один из распространенных видов пористых материалов - облицовочные звукопоглощающие материалы. Их изготавливают в виде плоских плит (плиты минераловатные «Акмигран», «Акмант», «Силаклор», «Винипор», ПА/С, ПА/О, ПП-80, ППМ, ПММ) или рельефных конструкций (пирамид, клиньев и т.д.), располагаемых или вплотную, или на небольшом расстоянии от сплошной строительной конструкции (стены, перегородки, ограждения и т.п.). Используются также звукопоглощающие облицовки из слоя пористо-волокнистого материала (стеклянного или базальтового волокна, минеральной ваты) в защитной оболочке из ткани или пленки с перфорированным покрытием (металлическим, гипсовым и др.).

Пористые звукопоглощающие материалы малоэффективны на низких частотах.

Отдельную группу звукопоглощающих материалов составляют резонансные поглотители. Они подразделяются на мембранные и резонаторные. Мембранные поглотители представляют собой натянутый холст (ткань), тонкий фанерный (картонный) лист, под которым располагают хорошо демпфирующий материал (материал с большой вязкостью, например, поролон, губчатую резину, строительный войлок и т.д.). В такого рода поглотителях максимум поглощения достигается на резонансных частотах.

Перфорированные резонаторные поглотители представляют собой систему воздушных резонаторов (например, резонаторов Гельмгольца), в устье которых расположен демпфирующий материал.

Средние значения звукоизоляции некоторых материалов приведены в таблице 4.5.

Повышение звукоизоляции стен и перегородок помещений достигается применением однослойных и многослойных (чаще - двойных) ограждений. В многослойных ограждениях целесообразно подбирать материалы слоев с резко отличающимися акустическими сопротивлениями (например, бетон - поролон).

Значения ослабления звука ограждениями, выполненными из некоторых часто применяемых строительных материалов, указаны в таблице 4.6.

**Таблица 4.5**

Звукопоглощающие свойства некоторых материалов

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Материал** | **Коэффициент поглощения на частотах, Гц** | | | | | |
| **125** | **250** | **500** | **1000** | **2000** | **4000** |
| Кирпичная стена | 0,024 | 0,025 | 0,032 | 0,041 | 0,049 | 0,07 |
| Деревянная обивка | 0,1 | 0,11 | 0,11 | 0,08 | 0,082 | 0,11 |
| Стекло одинарное | 0,03 | \* | 0,027 | \* | 0,02 | \* |
| Штукатурка известковая | 0,025 | 0,04 | 0,06 | 0,085 | 0,043 | 0,058 |
| Войлок (толщина 25 мм) | 0,18 | 0,36 | 0,71 | 0,8 | 0,82 | 0,85 |
| Ковер с ворсом | 0,09 | 0,08 | 0,21 | 0,27 | 0,27 | 0,37 |
| Стеклянная вата(толщиной 9 мм) | 0,32 | 0,4 | 0,51 | 0,6 | 0,65 | 0,6 |
| Хлопчатобумажная ткань | 0,03 | 0,04 | 0,11 | 0,17 | 0,24 | 0,35 |

Между помещениями зданий и сооружений проходит много технологических коммуникаций (трубы тепло-, газо-, водоснабжения и канализации, кабельная сеть энергоснабжения, вентиляционные короба и т.д.). Для них в стенах и перекрытиях сооружений делают соответствующие отверстия и проемы. Их надежная звукоизоляция обеспечивается применением специальных гильз, коробов, прокладок, глушителей, вязкоупругих заполнителей и т.д. Обеспечение требуемой звукоизоляции в вентиляционных каналах достигается использованием сложных акустических фильтров и глушителей.

Следует иметь в виду, что в общем случае звукоизоляция ограждающих конструкций, содержащих несколько элементов, должна оцениваться звукоизоляцией наиболее слабого из них.

**Таблица 4.6**

Звукопоглощающие свойства некоторых строительных конструкций

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Материал** | **Толщина** | **Звукоизоляция на частотах (Гц), дБ** | | | | | |
| **125** | **250** | **500** | **1000** | **2000** | **4000** |
| **Кирпичная стена** | 1/2 кирпича | 39 | 40 | 42 | 48 | 54 | 60 |
| **Отштукатуренная с двух сторон стена** | 1 кирпич | 36 | 41 | 44 | 51 | 58 | 64 |
| 1,5 кирпича | 41 | 44 | 48 | 55 | 61 | 65 |
| 2 кирпича | 45 | 45 | 52 | 59 | 65 | 70 |
| 2,5 кирпича | 47 | 55 | 60 | 67 | 70 | 70 |
| **Стена из железобетонных блоков** | 40 мм | 32 | 36 | 35 | 38 | 47 | 53 |
| 100 мм | 40 | 40 | 44 | 50 | 55 | 60 |
| 200 мм | 42 | 44 | 51 | 59 | 65 | 65 |
| 300 мм | 45 | 50 | 58 | 65 | 69 | 69 |
| 400 мм | 48 | 55 | 61 | 68 | 70 | 70 |
| 800 мм | 55 | 61 | 68 | 70 | 70 | 70 |
| **Стена из шлакоблоков** | 220 мм | 42 | 42 | 48 | 54 | 60 | 63 |
| Перегородка из древесно-стружечной плиты | 20 см | 23 | 26 | 26 | 26 | 26 | 26 |

Для того чтобы было невозможно прослушать конфиденциальный разговоры через стены с помощью стетоскопов используют генераторы акустического шума(например прибор виброакустической защиты SI-3001).

### Прибор виброакустической защиты SI-3001

|  |  |
| --- | --- |
|  | Защита помещений от прослушивания через строительные элементы конструкции. Принцип действия прибора основан на маскировании спектра речи шумовой помехой, излучаемой в стены, перекрытия, окна, воздуховоды, трубы отопления. |

ОСНОВНЫЕ ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ ПРИБОРА:

* Использование двух независимых каналов.
* Прибор имеет возможность подключения виброакустических излучателей отечественного и импортного производства (TRN-2000, OMS-2000, SPP-4.1, КВП и др.)
* Использование внутренней помехи, формируемой встроенным генератором и помехи подаваемой внешним источником сигнала (диктофон, генератор) на линейный вход прибора.
* Режим автоматического регулирования уровня сигнала на выходе прибора пропорционально уровню шума в защищаемом помещении.
* Регулировка уровня выходного сигнала в каждом канале, что позволяет настраивать прибор с разными типами датчиков под конкретные условия эксплуатации.
* Возможность плавной регулировки чувствительности микрофонного канала.
* Благодаря возможности подключения любых типов виброакустических излучателей потребитель может модифицировать имеющуюся систему защиты без демонтажа и замены ранее установленных излучателей.
* Прибор собран на современной импортной элементной базе ведущих фирм изготовителей и не имеет аналогов.

ТЕХНИЧЕСКИЕ ДАННЫЕ И ХАРАКТЕРИСТИКИ:

|  |  |
| --- | --- |
| Количество подключаемых излучателей: |  |
| электромагнитных (TRN-2000) | 72 |
| керамических (КВП-2) | 200 |
| акустических (OMS-2000) | 144 |
| пъезоизлучателей (SPP 4.1) | не ограничено |
| Спектр шумовой помехи | 25Гц ... 5 кГц |
| Номинальная выходная мощность | 70 Вт |
| Питание прибора электросеть | 220 В 50 Гц |
| Габаритные размеры | 200х215х53 мм |

Сертификат № 263 ГОСТЕХКОМИССИИ РОССИИ

Рекомендуется на одной защищаемой поверхности площадью до 10 кв.м. размещать один излучатель. На стеклах допускается приклеивать их в уголках, на стенах – лучше в середине.

Если подключить «гирлянду» датчиков-излучателей к прибору и включить его, то, приблизив ухо к защищаемой поверхности, можно услышать характерный шум. Если имеется стетоскоп, то попытка прослушать помещение убедительно покажет невозможность этого.

Для обнаружения радио стетоскопов можно использовать специальные приборы для обнаружения работающих радиопередатчиков.

#### “СРМ 700” Многофункциональный поисковый прибор

Портативный многофункциональный прибор СРМ-700 предназначен для выявления и локализации каналов утечки информации в широком диапазоне частот. Являясь одной из основных поисковых систем для комплексной защиты информации, выполняет пять наиболее важных функций:



**1.** При помощи высокочастотного зонда возможен поиск и обнаружение работающих радиопередатчиков, установленных в предметах интерьера, в одежде, в телефонных аппаратах и других технических средствах обработки и передачи данных. Прибор способен детектировать активизируемые передающие устройства с дистанционным управлением.

**2.** Низкочастотной антенной можно обследовать электро- и телефонные линии, а также провода электрической сети и кабели, которые могут являться каналами утечки информации.

**3.** При помощи высокочувствительного усилителя можно исследовать телефонные и другие линии на предмет выявления подключенных к ним микрофонов.

**4.** В режиме мониторинга прибор может быть использован для фиксации негласного включения передающих устройств с целью снятия информации.

**5.** Возможно подключение устройства звукозаписи для документирования всех выявленных сигналов.

Многофункциональный поисковый прибор **СРМ-700** легок и эффективен в работе благодаря автоматической регулировке усиления, цифровой регулировке режима работы. Благодаря высокой чувствительности СРМ-700 предназначен для быстрого и бесшумного детектирования всех основных типов электронных средств, предназначенных для скрытого получения информации. Прибор поставляется в атташе-кейсе. В качестве дополнительных аксессуаров предлагаются:

**IRP-700** — зонд инфракрасных излучений для обнаружения устройств, использующих ИК-лучи как средство передачи информации   
**MLP-700 —** зонд электромагнитных излучений   
**ALP-700** — акустический зонд   
**МРА-700** — телефонный адаптер   
**TRP-700** — шнур подключения к магнитофону   
**CLA-700** — адаптер питания от прикуривателя автомобиля   
**NCB-700** — комплект аккумуляторов   
**IRT-700** — тестовый инфракрасный передатчик   
**ССТ-700** — тестовый низкочастотный (сетевой) передатчик   
**ТТМ-700** — тестовый радиопередатчик

##### Технические характеристики:

|  |  |
| --- | --- |
| Диапазон частот ВЧ-антенны | 50 кГц – 3 ГГц |
| Чувствительность ВЧ-антенны | - 62 дБ на сегмент индикатора |
| Коэффициент усиления | 20 дБ |
| Диапазон частот НЧ-зонда | 15 кГц – 1 МГц |
| Чувствительность НЧ-зонда | - 38 дБ на сегмент индикатора |
| Максимальное входное напряжение | 300 В |
| Диапазон звуковых частот | 100 Гц – 15 кГц |
| Система отображения | 18-ти значный ЖКД |

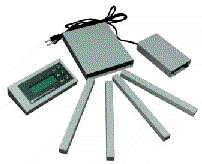
Для обнаружения стетоскопов с прямой записью на диктофон используют приборы для поиска диктофонов.

#### “PTRD-018” Стационарный обнаружитель диктофонов

PTRD - 018 (Portable tape recorder detector) - современная микропроцессорная система для защиты помещений от несанкционированного использования портативных звукозаписывающих устройств - диктофонов и им подобной аппаратуры. Система обеспечивает обнаружение работающего в режиме записи диктофона, определение его местоположения и времени работы с выводом текущей информации на ЖК-дисплей, либо через интерфейс RS-232 на экран монитора компьютера. Имеет раздельную индикацию по 16 независимым каналам, что позволяет более качественно оценивать угрозу несанкционированного применения звукозаписывающей аппаратуры.

##### Преимущества системы:

* Возможность обнаружения диктофонов в большом помещении - охват до 16 мест размеров порядка 1 ґ 1 м.



* Автоматическая адаптация к электромагнитной обстановке контролируемого помещения.
* Высокая защищенность от вибраций и электромагнитных помех.
* Применение жидкокристаллического дисплея обеспечивает наглядность результатов контроля: отображается номер канала, уровень сигнала, сообщение о тревоге.
* Обеспечение протоколирования результатов: все тревожные события, произошедшие за время сеанса контроля, заносятся в протокол с указанием номера канала, частоты сигнала, его уровня, времени включения и выключения.
* Возможность выбора режимов работы в зависимости от поставленной задачи: "быстрее" или "дальше".
* Возможность подключения к компьютеру позволяет интегрировать PTRD-018 в общую систему безопасности.

##### Принцип действия:

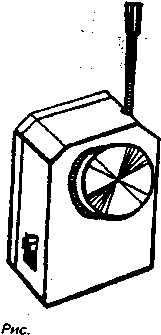
Основой построения системы является регистрация электромагнитных полей, создаваемых работающим мотором диктофонов. При появлении в контролируемой зоне работающего диктофона, он обнаруживается системой и индицируется сигналом тревоги. Контроль каналов повторяется последовательно, и результаты контроля оперативно отображаются на дисплее.

##### Технические характеристики:

|  |  |
| --- | --- |
| Дальность обнаружения в зависимости от типа диктофона | от 0,5 до 1,5 м |
| Число каналов | 4, 8, 16 |
| Время обнаружения | не более 30 секунд на канал |

**8.Стетоскопы**

Стетоскоп представляет собой вибродатчик, усилитель и головные те­лефоны. Схема применения стетоскопа приведена на рис.



Вибродатчик специальной мастикой прикрепляется к стене, потолку и т.п. Размеры датчика, на примере устройства БТ1, составляют 2,2x0,8 см, диапазон частот — 300-3000 Гц, вес — 126 г, коэффициент усиления — 20000.

С помощью подобных устройств можно осуществлять прослушивание разговора через стены толщиной до 1 м. Стетоскоп может оснащаться проводным, радио или другим каналом передачи информации. Основ­ным преимуществом стетоскопа можно считать трудность обнаружения, т.к. он может устанавливаться в соседних помещениях.

В качестве примера приведем два устройства — 51РЕ К5 и 51РЕ ОРТО2000, отличающиеся каналом передачи. Микрофон-стетоскоп раз­мером 2x3 см обеспечивает прослушивание через стены толщиной до 50 см и оконные рамы с двойными стеклами. Мощность передатчика 51РЕ КЗ — 20 мВт, дальность — 250 м. Размеры передатчика составляют 44x32x14 мм, масса — 41 г, время непрерывной работы — 90 часов. ИК система 51РЕ ОРТО 2000 обеспечивает радиус действия 500 м и имеет широкую диа­грамму направленности.

Существуют стетоскопы, в которых чувствительный элемент, усилитель и радиопередатчик объединены в одном корпусе. Имеющий очень небольшие габари­ты, радиостетоскоп достаточно прикрепить с помощью специальной липкой массы к стене, полу или потолку в соседнем помещении. В качестве примера такого стетоскопа на рис. 1.25 изображен стетоскоп АД-50.

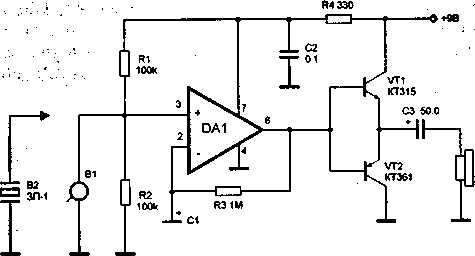
Этот компактный стетоскоп позволяет не только прослушивать разговоры через стены, оконные рамы, двери, но и передавать инфор­мацию по радиоканалу. Имеет высокую чув­ствительность и обеспечивает хорошую разбор­чивость речевого сигнала. Рабочая частота со­ставляет 470 МГц. Дальность передачи — до 100 м. Время непрерывной работы — 24 ч, размеры — 40x23 мм.

**Микрофон-стетоскоп**

Наряду с узконаправленными и проводными выносными микрофонами, существуют устройства, которые регистрируют вибрацион­ные колебания стен, потолков, стекол, вентиляционных шахт и т. д. Эти устройства называются микрофоны-стетоскопы. Они представ­ляют собой довольно сложные устройства. Поэтому ниже описано устройство, которое может служить прообразом микрофона-стетоско­па, и принцип его работы. Принципиальная схема устройства приво­дится на рис. 2.45.

Усилитель звуковой частоты собран на микросхеме DА1 типа К140УД6. Резисторы R1 и R2 задают режим работы микросхемы. Коэффициент усиления определяется значением сопротивления резис­тора RЗ. Транзисторы VТ1 типа КТ315 и VТ2 типа КТ361 включены по схеме эмиттерных повторителей и усиливают выходной сигнал по току. Нагрузкой усилителя служат головные телефоны ТЭМ-2.

Датчик вибрации делается из пьезокерамической головки В1, сня­той со старого проигрывателя. Виброколебания преобразуются пьезодатчиком в электрические и усиливаются усилителем ВА1. В качестве пьезодатчика В2 можно применить пьезоизлучатель типа ЗП-1, ЗП-22 и им подобные от электронных часов и игрушек. Они хорошо воспро­изводят частоты в диапазоне 800-3000 Гц, что, в основном, перекры­вает речевой диапазон частот. При необходимости можно усилить сигнал до нужной величины, используя дополнительный усилитель звуковой частоты. Сигнал на него поступает с выхода операционного усилителя DА1. Подобный датчик может быть с успехом использован и в качестве датчика охран­ной сигнализации. В качестве пьезодатчика В1 можно использовать, например, ПЭ-1, ГЗП-308 и другие.



**Вывод**

Преимуществом этой схемы является простота исполнения и дешевизна элементов, а также то, что питание её можете осуществлятся от гальванического элемента питания с напряжением питания 9В. Не достаток то, что для прослушивания конфиденциальных разговоров с помощью её нужно непосредственно быть рядом, во избежании этого можно вместо громкоговорителя подключить звукозаписывающее устройство, впоследствии подключение которого габариты прибора увеличатся.

**9. Заключение**

В данной курсовой работе рассмотрена комплексная система защиты информационных ресурсов объекта – кабинета руководителя предприятием. Изложены основные сведения, которые требуются для организации такой защиты. Среди них и теоретическая база, и практические решения информационной безопасности такие как: выявление каналов утечки информации и их защита, способов несанкционированного доступа и их предотвращение (второй раздел), модели угроз и приемы их реализации (третий пункт).

Главной целью злоумышленника является получение информации о составе, состоянии и деятельности объекта конфиденциальных интересов (фирмы, изделия, проекта, рецепта, технологии и т.д.) в целях удовлетворения своих информационных потребностей. Возможно в корыстных целях и внесение определенных изменений в состав информации, циркулирующей на объекте конфиденциальных интересов. Такое действие может привести к дезинформации по определенным сферам деятельности, учетным данным, результатам решения некоторых задач. Более опасной целью является уничтожение накопленных информационных массивов в документальной или магнитной форме и программных продуктов. Полный объем сведений о деятельности конкурента не может быть получен только каким-нибудь одним из возможных способов доступа к информации. Чем большими информационными возможностями обладает злоумышленник, тем больших успехов он может добиться в конкурентной борьбе. На успех может рассчитывать тот, кто быстрее и полнее соберет необходимую информацию, переработает ее и примет правильное решение. От целей зависит как выбор способов действий, так и количественный и качественный состав привлекаемых сил и средств посягательства.

Точно также, способы защиты информационных ресурсов должны представлять собой целостный комплекс защитных мероприятий, планирование которых рассмотрено в четвертом и пятом разделах. Разумеется, это не полный перечень, поскольку каждый руководитель решает какие методы и средства защиты необходимо использовать применительно к данному объекту, что зависит от функций, выполняемых объектом, а также от его экономических соображений. Таким образом, главной целью данной курсовой работы была разработка комплексной системы защиты информации.

**Список литературы**

1. Волокитин А.В., Маношкин А.П., Солдатенков А.В., Савченко С.А., Петров Ю.А. Информационная безопасность государственных организаций и коммерческих фирм. Справочное пособие (под общей редакцией Реймана Л.Д.) М.: НТЦ «ФИОРД-ИНФО», 2002г.-272с.
2. Шпионские страсти. Электронные устройства двойного применения. Рудометов Е.А. четвертое издание 2000г.
3. Петраков А.В. Основы практической защиты информации. 3-е изд. Учебное пособие-М.: Радио и связь, 2001г.-368с.
4. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации(под редакцией Ковтанюка) К.: Издательство Юниор, 2003г.-504с.
5. WEB-сайт www.razvedka.ru