Белорусский государственный университет

Информатики и радиоэлектроники

Кафедра РЭС

Реферат

На тему:

"**Методы и средства защиты информации**"

**Минск 2008**

**Методы защиты информации.**

**Установка препятствия** — метод физического преграждения пути злоумышленнику к защищаемой информации, в т.ч. попыток с использованием технических средств съема информации и воздействия на нее.

**Управление доступом** — метод защиты информации за счет регулирования использования всех информационных ресурсов, в т.ч. автоматизированной информационной системы предприятия. Управление доступом включает следующие функции защиты:

• идентификацию пользователей, персонала и ресурсов информационной системы (присвоение каждому объекту персонального идентификатора);

• аутентификацию (установление подлинности) объекта или субъекта по предъявленному им идентификатору;

• проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);

• разрешение и создание условий работы в пределах установленного регламента;

• регистрацию (протоколирование) обращений к защищаемым ресурсам;

• реагирование (сигнализация, отключение, задержка работ, отказ в запросе) при попытках несанкционированных действий.

**Маскировка** — метод защиты информации с использованием инженерных, технических средств, а также путем криптографического закрытия информации.

Маскираторы аналогово-цифровые статические.

Скремблеры - маскираторы аналогово-цифровые динамические.

Вокодеры - устройства, передающие речь в цифровом виде и зашифрованном.

Методы защиты информации на практике реализуются с применением средств защиты.

**Средства защиты информации.**

Средства защиты информации можно разделить на:

1. Средства, предназначенные для защиты информации. Эти средства не предназначены для непосредственной обработки, хранения, накопления и передачи защищаемой информации, но находящиеся в одном помещении с ними.

Делятся на:

пассивные – физические (инженерные) средства, технические средства обнаружения, ОС, ПС, СКУД, ВН, приборы контроля радиоэфира, линий связи и т.п.;

активные – источники бесперебойного питания, шумогенераторы, скремблеры, устройства отключения линии связи, программно-аппаратные средства маскировки информации и др.

2. Средства, предназначенные для непосредственной обработки, хранения, накопления и передачи защищаемой информации изготовленные в защищенном исполнении. НИИЭВМ РБ разрабатывает и выпускает защищенные носимые, возимые и стационарные ПЭВМ.

3. Средства, предназначенные для контроля эффективности защиты информации.

**Пассивные средства защиты акустического и виброакустического каналов утечки речевой информации**.

Для предотвращения утечки речевой информации по акустическому и виброакустическому каналам осуществляются мероприятия по выявлению каналов утечки. В большинстве случаев для несанкционированного съема информации из помещения противник применяет соответствующие замыслу закладные устройства.

Всю процедуру поиска ЗУ можно условно разбить на несколько этапов:

• физический поиск и визуальный осмотр;

• обнаружение радиозакладных устройств как электронных средств;

• проверка наличия каналов утечки информации.

**Физический поиск и визуальный осмотр.**

Осмотр осуществляется путем обследования всех предметов в зоне контроля, размеры которых достаточно велики для того, чтобы можно было разместить в них технические средства негласного съема информации (настольные приборы, рамы картин, телефоны, цветочные горшки, книги, питаемые от сети устройства: компьютеры, ксероксы, радиоприемники и т. д.).

Физический поиск и визуальный осмотр объектов проводят с применением специальных средств видеонаблюдения и металлодетекторов.

**Обнаружение радиозакладных устройств (РЗУ).**

Необнаруженных при визуальном осмотре осуществляют по их демаскирующим признакам с применением специальных средств обнаружения. РЗУ, как правило, содержат в своей конструкции электронные схемы и, при своей работе излучают радиосигнал.

Основными признаками излучения радиозакладок являются:

* относительно высокий уровень излучения, обусловленный необходимостью передачи сигнала за пределы контролируемого помещения.
* непрерывная или непрерывная в течение некоторого времени работа (прерывистый режим работы днем и практически, полное молчание ночью; излучение возникает одновременно с поднятием трубки и исчезает, когда трубка положена).
* появление нового источника в обычно свободном частотном диапазоне.
* использование в ряде радиозакладок направленных антенн приводит к сильной локализации излучения, то есть существенной неравномерности его уровня в пределах контролируемого объекта.
* особенности поляризации излучения радиозакладок. При изменении пространственного положения или ориентации приемной антенны наблюдается изменение уровня всех источников. Однако однотипные удаленные источники одного диапазона ведут себя примерно одинаково, тогда как сигнал закладки изменяется отлично от остальных. Эффект поляризации обнаруживается при использовании анализаторов спектра.
* изменение («размывание») спектра излучений радиомикрофонов при возникновении каких-либо шумов в контролируемом помещении. Он проявляется только в том случае, если РЗУ работает без кодирования передаваемой информации.

К основным устройствам, применяемым для обнаружения РЗУ относятся:

- индикаторы поля;

- специальные радиоприемники;

- программно-аппаратные комплексы радиоконтроля;

- нелинейные радиолокаторы.

Индикаторы поля – приборы определяющие наличие ЗУ по их радиоизлучению. Индикаторы, или детекторы поля являются простейшими средствами обнаружения факта использования радиозакладок. Это приемники с низкой чувствительностью, поэтому они обнаруживают излучения радиозакладных устройств на предельно малых расстояниях (10-40 см), чем и обеспечивается селекция «нелегальных» излучений на фоне мощных «разрешенных» сигналов. Важное достоинство детекторов - способность находить передающие устройства вне зависимости от применяемой в них модуляции. Основной принцип поиска состоит в выявлении абсолютного максимума уровня излучения в помещении.

Иногда детекторы используют и в так называемом сторожевом режиме. В этом случае после полной проверки помещения на отсутствие ЗУ фиксируется уровень поля в некоторой точке пространства (обычно это стол руководителя или место ведения переговоров), и прибор переводится в дежурный режим. В случае включения закладки (примерно на удалении до двух метров от детектора), индикатор выдает сигнал о повышении уровня электромагнитного поля. Однако необходимо учитывать тот факт, что если будет использоваться радиозакладка с очень низким уровнем излучения, то детектор скорее всего не зафиксирует ее активизацию.

Специальные радиоприемные устройства.

Радиоприемные устройства, как устройства выявления радиозакладок, должны удовлетворять трем основным условиям:

• иметь возможность настройки на частоту работы устройств, скрытно передающихперехваченную информацию, т.е. иметь возможность контролировать большой набор частот либо одновременно во всем диапазоне либо перестраиваясь от значения к значению за предельно малый промежуток времени - панорамные приемники;

• обладать функциями выделения нужного сигнала по характерным признакам на фоне мешающих сигналов и помех (избирательность по спектру частот);

• обладать способностью к демодуляции различных видов сигналов (избавляться от сигнала несущей частоты, а полезный сигнал преобразовывать в низкочастотный сигнал и демодулировать с помощью детектора, соответствующего типу использованной модуляции).

**Программно-аппаратные комплексы радиоконтроля.**

Для расширения возможностей специальных приемников их функционально совмещают с персональными компьютерами, что существенно повышает надежность и оперативность поиска ЗУ, делает процедуру выявления более удобной (технологичной).

На компьютер при этом возлагается решение следующих задач:

• хранение априорной информации о радиоэлектронных средствах, работающих в контролируемой области пространства и выбранных диапазонах частот;

• получение программными методами временных и частотных характеристик принимаемых сигналов;

• тестирование принимаемых сигналов по совокупности признаков на принадлежность к излучению ЗУ.

Программно-аппаратные комплексы радиоконтроля обеспечивают:

• выявление излучений РЗУ;

• пеленгование РЗУ в реальном масштабе времени;

• определение дальности до источников излучения;

• аналого-цифровую обработку сигналов с целью определения их принадлежности к излучению РЗУ;

• контроль силовых, телефонных, радиотрансляционных и других сетей;

• работу в многоканальном режиме, позволяющем контролировать несколько объектов одновременно;

• постановку прицельных помех на частотах излучения РЗУ и др.

Программно-аппаратные комплексы радиоконтроля состоят из следующих элементов:

• широкодиапазонного перестраиваемого по частоте приемника (сканера);

• блока распознавания РЗУ, осуществляющего идентификацию излучений радиомикрофонов на основе сравнения принятых детектированных сигналов с естественным акустическим фоном помещения (пассивный способ) или тестовым акустическим сигналом (активный способ);

• блока акустической локации, позволяющего по запаздыванию переизлученного зондирующего звукового импульса определять расстояние до активных радиомикрофонов;

• электронно-вычислительной машины (процессора), осуществляющей как обработку полученных данных, так и управление приемником.

По принципу построения все известные приборы данного класса делятся на две основные группы:

• специально разработанные комплексы, конструктивно выполненные в виде единого устройства;

• комплексы, сформированные на базе серийного сканера, персонального компьютера (обычно notebook) и специального программного обеспечения.

Нелинейные радиолокаторы.

Применяются для поиска внедренных РЗУ, не использующих радиоканал для передачи информации, а также РЗУ, находящихся в пассивном (неизлучающем) состоянии.

Нелинейные радиолокаторы - приборы, излучающие электромагнитную волну с частотой f, а принимающие переизлученные сигналы на частотах f. Если такие сигналы будут обнаружены, то в зоне действия локатора есть полупроводниковые элементы, и их необходимо проверить на возможную принадлежность к ЗУ. Нелинейный радиолокатор обнаруживает только радиоэлектронную аппаратуруи, в отличие от классического линейного радиолокатора, «не видит» отражений от окружающих предметов, то есть обладает высокой избирательностью. Источниками помех для его работы могут служить контакты со слабым прижимом, для которых характерно наличие промежуточного окисного слоя.

**Активные технические средства защиты акустического и виброакустического канала.**

Для активной защиты речевой информации от необнаруженных закладных устройств и съема по другим каналам используется аппаратура активной защиты:

* Технические средства пространственного зашумления;
* Устройства виброакустической защиты;
* Технические средства ультразвуковой защиты.

##### Технические средства пространственного и линейного зашумления.

По принципу действия все технические средства пространственного и линейного зашумления можно разделить на три большие группы:

средства создания акустических маскирующих помех:

* генераторы шума в акустическом диапазоне;
* устройства виброакустической защиты;
* технические средства ультразвуковой защиты помещений;

средства создания электромагнитных маскирующих помех:

* технические средства пространственного зашумления;
* технические средства линейного зашумления, которые в свою очередь делятся на средства создания маскирующих помех в коммуникационных сетях и средства создания маскирующих помех в сетях электропитания;
* многофункциональные средства защиты.

**Генераторы шума в акустическом диапазоне.**

Основной принцип радиоэлектронного противодействия - создание помех для приемного устройства с интенсивностью, достаточной для нарушения его работы.

Если заранее неизвестна его рабочая частота, то необходимо создать помеху по всему возможному или доступному диапазону спектра. Достаточно универсальной помехой для связных радиолиний считается шумовой сигнал. В связи с этим аппаратура радиопротиводействия должна включать в свой состав генератор шума достаточной мощности (на необходимый диапазон) и антенную систему. Практически при отношении верхней и нижней частоты диапазона более 2-х используют несколько шумовых генераторов и комбинированную многодиапазонную антенну.

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

Примерный вид структурной схемы источника акустического шума приведен на рис.1. Конструктивно аппаратура включает блок формирования и усиления шумового сигнала и несколько акустических излучателей.

Излучатель акустического шума № 1

Генератор шума

Излучатель акустического шума №.Х

Рис.1. Структурная схема источника акустического шума

В некоторых случаях наличие нескольких излучателей необязательно. Тогда используются компактные генераторы со встроенной акустической системой, акустический генератор белого шума.

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

Устройства виброакустической защиты.

Устройства виброакустической защиты используются для защиты помещений, предназначенных для проведения конфиденциальных мероприятий, от съема информации через оконные стекла, стены, системы вентиляции, трубы отопления, двери и т.д. Данная аппаратура позволяет предотвратить возможное прослушивание с помощью проводных микрофонов, звукозаписывающей аппаратуры, радиомикрофонов и электронных стетоскопов, лазерного съема акустической информации с окон и т.д. Противодействие прослушиванию обеспечивается внесением виброакустических шумовых колебаний в элементы конструкции здания.

Конструктивно аппаратура включает блок формирования и усиления шумового сигнала и несколько акустических и виброакустических излучателей (рис.2). Генератор формирует «белый» шум в диапазоне звуковых частот. Передача акустических колебаний на ограждающие конструкции производится при помощи пьезоэлектрических (на основе пьезокерамики) или электромагнитных вибраторов с элементами крепления. Конструкция и частотный диапазон излучателей должны обеспечивать эффективную передачу вибрации. Вибропреобразователи возбуждают шумовые виброколебания в ограждающих конструкциях, обеспечивая при этом минимальный уровень помехового акустического сигнала в помещении, практически не влияющий на комфортность проведения переговоров.

Предусмотренная в большинстве изделий возможность подключения акустических излучателей, позволяет «зашумлять» вентиляционные каналы и дверные тамбуры. Как правило, имеется возможность плавной регулировки уровня шумового акустического сигнала. При этом надо ориентироваться на то, что восстановить перехваченное сообщение практически невозможно, если уровень помехи более чем в 10 раз превышает уровень сигнала во всем частотном диапазоне (отношение сигнал/помеха менее - 20 дБ).

Генератор шума

Излучатель виброколебаний № 1

Излучатель виброколебаний №...

Излучатель акустического шума № 1

Излучатель акустического шума №...

Рис. 2. Структурная схема устройства виброакустической защиты

Технические средства ультразвуковой защиты помещений.

Отличительной особенностью технических средств УК защиты является воздействие на микрофонное устройство и его усилитель достаточно мощным ультразвуковым сигналом (группой сигналов), вызывающим блокирование усилителя или возникновение значительных нелинейных искажений, приводящих, в конечном счете, к нарушению работоспособности микрофонного устройства (его подавлению).

Поскольку воздействие осуществляется по каналу восприятия акустического сигнала, то совершенно не важны его дальнейшие трансформации и способы передачи. Акустический сигнал подавляется именно на этапе его восприятия чувствительным элементом. Все это делает комплекс достаточно универсальным по сравнению с другими средствами активной защиты. При этом не происходит существенного снижения эргономических характеристик помещения.

**Многофункциональные средства защиты.**

При практической организации защиты помещения от утечки информации по техническим каналам необходимо комплексное использование различных устройств безопасности: акустических, виброакустических, сетевых генераторов шума и источников электромагнитного маскирующего излучения. При этом можно пойти следующими тремя путями:

* подбором различных устройств защиты информации и их автономным использованием;
* объединением различных устройств защиты информации в единый комплекс путем применения универсального блока управления и индикации;
* использованием готовых комплектов.

**Литература:**

1**.** Барсуков В.С. Безопасность: технологии, средства, услуги / В.С. Барсуков. – М., 2001 – 496 с.

2. Ярочкин В.И. Информационная безопасность. Учебник для студентов вузов / 3-е изд. – М.: Академический проект: Трикста, 2005. – 544 с.

3. Барсуков В.С. Современные технологии безопасности / В.С. Барсуков, В.В. Водолазский. – М.: Нолидж, 2000. – 496 с., ил.

4. Зегжда Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко. - М.: Горячая линия – Телеком, 2000. - 452 с., ил.

5. Компьютерная преступность и информационная безопасность / А.П. Леонов [и др.]; под общ. Ред. А.П. Леонова. – Минск: АРИЛ, 2000. – 552 с.