БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Кафедра РЭС

РЕФЕРАТ

На тему:

"Условия и причины образования технических каналов утечки речевой информации"

МИНСК, 2008

Речевая информация – информация, распространение которой осуществляется посредством звуковых (акустических), вибрационных, электромагнитных сигналов. Люди говорят друг с другом непосредственно и используют для общения средства связи.

Речь характеризуется (полученный речевой сигнал):

* разборчивостью – отношением числа правильно понятых элементов речи (звуков, слогов, слов) к общему числу принятых элементов;
* реверберацией звука – эффектом наложения речевых отрезков друг на друга в результате отражения сигнала от поверхностей конструкций;
* ослаблением звуковых колебаний – при прохождении речевых сигналов через различные среды (бетон, кирпич, стекло, воздух, вода …);
* присутствием шумов и помех – в месте возникновения речевой информации и по пути ее следования к пункту приема.

## Средства разведки

Условиями для образования утечек в среде, окружающей источник речевой информации могут являться наличие в ней:

* акустических и виброаккустических колебаний;
* радио-, оптических и электрических сигналов, содержащих сведения, в различных технических средствах обработки и передачи информации;
* нежелательных электромагнитных излучений систем и средств информатизации и связи;
* наводок электромагнитных излучений на различные токоведущие цепи и конструкции;
* специальных воздействий на элементы технических средств;
* различных закладных устройств;
* случайных электроаккустических преобразователей в отдельных элементах технических средств.

В окружающей среде возникают виброакустические, гидроакустические, акустоэлектрические, электрические (в телефонной линии) сигналы, электромагнитные сигналы в эфире (разговор по радиотелефону), побочные электромагнитные излучения и наводки. Акустическая энергия, возникающая при разговоре, может вызвать акустические (механические) колебания элементов электронной аппаратуры, что, свою очередь, приводит появлению новых или изменению существующих электромагнитных сигналов.

Утечка информации по аккустическим и виброаккустическим каналам.

Различают прямой аккустический канал - подслушивание (прямой перехват акустических колебаний в диапазоне частот от 16-25Гц до 18…20 КГц) и канал с применением микрофонов, преобразующих акустические колебания в электрические сигналы.

Наиболее простым способом перехвата речевой информации является подслушивание (прямой перехват). Разведываемые акустические сигналы могут непосредственно приниматься ухом человека, реагирующим на изменение звукового давления, возникающего при распространении звуковой волны в окружающем пространстве. Диапазон частот акустических колебаний, слышимых человеком, простирается от 16...25Гцдо 18... 20 кГц в зависимости от индивидуальных особенностей слушателя. Человек воспринимает звук в очень широком диапазоне звуковых давлений. Одной из опорных величин этого диапазона является стандартный порог слышимости. Под ним условились понимать эффективное значение звукового давления, создаваемое гармоническим звуковым колебанием частоты F= 1000 Гц, едва слышимым человеком со средней чувствительностью слуха. Порогу слышимости соответствует звуковое давление Рзв0 = 2-10~5 Па. Верхний предел определяется значением Pзв = 20 Па, при котором наступает болевое ощущение (стандартный порог болевого ощущения).

В случаях, когда уровни звукового давления, создаваемого звуковой волной, ниже порога слышимости, когда нет возможности непосредственно прослушивать речевые сообщения или когда требуется их зафиксировать (записать), используют микрофон.

Микрофон является преобразователем акустических колебаний в электрические сигналы. В зависимости от физического явления, приводящего к такому преобразованию, различают основные типы микрофонов:

- электродинамические;

- электромагнитные;

- электростатические;

- пьезоэлектрические;

- магнитострикционные;

- контактные и т.д.

Действие электродинамического преобразователя основано на использовании явления электромагнитной индукции. В кольцевом зазоре 1 магнитной системы, имеющей постоянный магнит 2, находится подвижная катушка 3, соединенная с диафрагмой 4. При воздействии на диафрагму 4 звукового давления, она вместе с подвижной катушкой 3 совершает колебания в магнитном поле, создаваемом магнитной системой 2. В витках катушки 3, пересекающих магнитные силовые линии, возникает напряжение, являющееся выходным сигналом микрофона.

Структурная схема для иллюстрации прямого канала и канала с применением микрофона для перехвата акустической информации выглядит следующим образом:

Причины, приводящие к применению прямого канала утечки информации:

Микрофон

Усилитель

Наушники

Магнитофон

Проводной канал

Радиоканал

Оптический и др.каналы

Отсутствие или недостатки режима безопасности;

Неадекватный обстановке подбор по функциональным возможностям технических средств защиты.

Некачественное обслуживание технических средств и систем защиты, отказ в работе.

Недостатки в работе с персоналом объекта.

Высокопрофессиональные действия "нарушителя".

Утечка информации по виброаккустическим каналам.

Как известно, виброаккустический канал создается за счет преобразования акустических колебаний в воздушной среде в вибрационные колебания в твердой среде, окружающей данную воздушную среду.

Обобщенная структурная схема виброаккустического канала может быть представлена следующим образом:

Условия и причины утечки речевой информации в различных средах и в технических средствах обработки и передачи информации.

Вибродатчик

Усилитель

Наушники

Магнитофон (устройство регистрации и воспроизвед.)

Проводной канал

Радиоканал

Оптический и др.каналы

Твердая среда

1) Перехват разговоров по радиотелефонам, сотовой и пейджинговой связи.

Комплекс технических средств электрорадиосвязи на любой территории включает в себя первичную сеть каналов (кабель, волновод, связь через ИСЗ и т.д.) и построенные на его базе вторичные сети, предназначенные для удовлетворения потребностей в передаче любых сообщений (телефонных, электронной почты, телевизионных и др.).

Превращение сообщения в сигнал состоит из трех операций, которые могут быть независимыми или совмещенными:

* преобразование – превращение неэлектрических величин, соответствующих первоначальному сообщению в электрические величины.
* кодирование – построение сигнала по некоторому определенному принципу, имеющему обычно сравнительно несложное математическое выражение (код Морзе, …код Бодо, приемы криптографии);
* модуляция – воздействие на какой-либо параметр переносчика сигналом сообщения, в результате чего в изменениях этого параметра оказывается присутствующим передаваемый сигнал.
* амплитудная модуляция (АМ);
* частотная модуляция (ЧМ);
* фазовая модуляция (ФМ).

В современных системах связи, где переносчиком является периодическая последовательность коротких импульсов, различают;

АИМ – амплитудно-импульсная модуляция – модуляция последовательности импульсов по высоте;

ДИМ – модуляция по длительности импульсов;

ФИМ – модуляция по фазе импульсов;

ЧИМ – модуляция по частоте импульсов;

ИКМ – импульсно-кодовая модуляция.

Существуют:

Основное радиоизлучение – излучение радиопередающего устройства в необходимой полосе радиочастот.

Необходимая полоса радиочастот – минимальная полоса частот данного класса радиоизлучения, достаточная для передачи сигнала с требуемой скоростью и качеством.

К нежелательным радиоизлучениям радиопередающих устройств относят радиоизлучения за пределами необходимой полосы радиочастот:

* внеполосные - нежелательные радиоизлучения в полосе частот, примыкающей к необходимой полосе радиочастот, являющиеся результатом модуляции. Они могут быть вызваны наличием нелинейностей в модулирующей части радиопередающего устройства и другими причинами.
* побочные – побочные излучения на гармониках, субгармониках, паразитные, комбинационные и интермодуляционные. Возникают в результате нелинейных процессов в передатчике, фидере, антенном устройстве радиопередающего устройства. Могут возникать из-за воздействия на радиопередающее устройство внешних электромагнитных полей.
* шумовые – обусловлены собственными шумами и паразитной модуляцией генерируемого колебания шумовыми процессами радиопередатчика.

Перехват разговоров по радиотелефонам не представляет трудности. Достаточно настроить приемник (сканер) на частоту несущей радиотелефона, находящегося в зоне приема и установить соответствующий режим модуляции. Например, телефонные аппараты типа ТА-Т, ТА-12, ТА-32 с кнопочным номеронабирателем при наборе номера и при ведении переговоров излучают информацию на десятках частот в средневолновом, коротковолновом и ультракоротком диапазонах. Это излучение может быть зарегистрировано на расстоянии до 200м. У телефонов с радиоудлинителем радиус перехвата без спецзакладок достигает 800м. Перехват излучений может осуществляться с помощью малогабаритного индуктивного датчика, позволяющего улавливать побочные электромагнитные колебания практически любого телефонного аппарата даже с расстояния 1м.

Для перехвата переговоров, ведущихся по мобильной сотовой связи необходимо использовать более сложную аппаратуру. в настоящее время существуют различные комплексы контроля сотовой системы связи стандартов AMPS, DAMPS, NAMPS, NMT-450, NMT-450i, разработанных и изготовленных в России и странах Западной Европы.

Комплексы позволяют обнаруживать и сопровождать по частоте входящие и исходящие звонки абонентов сотовой связи, определять входящие и исходящие номера телефонов абонентов, осуществлять слежение по частоте за каналом во время телефонного разговора, в том числе при переходе из соты в соту. Количество задаваемых для контроля абонентов определяется составом аппаратуры комплекса и версией программного обеспечения и может достигать до 16 и более. Комплексы позволяют вести автоматическую запись переговоров на диктофон, вести на жестком диске ПЭВМ протокол записей на диктофон, осуществлять полный мониторинг всех сообщений, передаваемых по служебному каналу, а также определять радиослышимость всех базовых станций в точке их приема с ранжировкой по уровням принимаемых от базовых станций сигналов.

Стандарт GSM (Groupe Speciale Mobile), разработанный Европейским институтом телекоммуникационных стандартов (European Telecommunications Standard institute), на сегодняшний день является самым распространенным в мире - он используется в 79 млн. сотовых аппаратов, преимущественно в странах Европы и Азии. До сих пор считалось, что телефоны GSM обладают столь надежной защитой, что их нельзя не только прослушать, но и размножить, то есть сделать несколько аппаратов, одновременно пользующихся одним и тем же номером. Но, увы!

Зашифрованные данные абонента GSM хранятся в небольшой смарт-карте, которая вставляется в телефон. Без карты, называемой также модулем идентификации пользователя (SIM - Subscriber Identification Module), аппарат представляет собой бесполезную оболочку. Карту, идентифицирующую владельца, можно использовать с любым стандартным телефоном. Обнаруженная дыра в безопасности позволяет извлечь секретную информацию из одного SIM и переписать ее в другой, создав точную копию первого телефона.

2) Утечки в проводных и оптоволоконных линиях передачи информации.

Утечки информации через проводные и оптоволоконные линии передачи информации могут происходить по разным причинам. Однако во всех случаях должен присутствовать "нарушитель" оснащенный соответствующими приборами. Линии могут быть телефонные, радиосети, охранной и пожарной сигнализации, электропитания и заземления и т.п. .

Рассмотрим строение телефонной линии связи. По системе построения телефонные линии разделяют на шкафные и бесшкафные, по условиям прокладки – на подземные в специальной телефонной канализации, подземные в коллекторах и тоннелях, подземные бронированные, подводные, воздушные стечные, воздушные столбовые, настенные открытой и скрытой прокладки, и др.

Основные зоны перехвата речевой информации, передаваемой по телефонным линиям:

Зона "А" – сам телефонный аппарат (ТА);

Зона "Б" – путь сигнала от ТА к РК (распределительной коробке);

Зона "В" – распределительный кабель от РК к РШ (распределительный шкаф) включая саму РК и РШ и магистральный кабель от РШ до АТС;

Зона "Г" - АТС;

Зона "Д" – линии связи между АТС

**ТА**

**РК**

АТС

АТС

**РШ**

 А Б Б В В В Д

 До 3 км. Г Г

Зона А. В телефонный аппарат может быть установлено закладное устройство, а также могут быть использованы конструктивные элементы, входящие в состав телефонного аппарата. Отдельные конструкции телефонных аппаратов создают вокруг себя различные излучения, которые также могут быть использованы для несанкционированного съема информации.

Зона Б. Является наиболее удобной для доступа к определенной линии. Несанкционированный съем информации в данной зоне может осуществляться как с непосредственным подключением к линии, так и индуктивным способом. Телефонная линия может также использоваться в качестве проводника, по которому передается снимаемая информация.

Подключение к телефонной линии может осуществляться следующими способами:

Непосредственное подключение. Слушать можно, начиная с параллельного телефона, специальной монтерской трубки, записывать на диктофон, магнитофон, в память компьютера. Можно подключать специальные устройства для съема информации с телефонной линии и окружающего объема.

Съем информации с ТЛ при последовательном подключении через согласующее устройство с полной компенсацией изменения напряжения.

Съем информации с ТЛ при параллельном подключении через согласующее устройство с полной компенсацией изменения напряжения.

Съем телеграфных сообщений факсимильных Без непосредственного подключения к линии. Подключение бесконтактным способом. Подключение с помощью индуктивного датчика, выполненного в виде трансформатора, расположенного вблизи телефонной линии. Но здесь требуется усилитель звуковой частоты с автономным питанием.

Съем индукционным способом Зона В. Здесь уже существует проблема поиска нужной линии. Требуется спецоборудование для вычленения нужной линии.

Зона Г. Поиск необходимой линии в зоне Г не представляет трудности, но АТС является объектом с ограниченным доступом и установить в данной зоне оборудование для съема информации разрешается только по решению Прокурора. Контроль на АТС может осуществляться выборочно и совершенно свободно. Ведомственная АТС также может использоваться для контроля переговоров своих сотрудников. Рынок предлагает специальные многоканальные стационарные устройства записи телефонных переговоров от 1 до 100 каналов одновременно.

Зона Д. Для съема информации в данной зоне требуется дорогостоящее оборудование и высокая квалификация специалистов. Однако перехват возможен, хотя и связки кабелей снабжены защитой. Система "Крот", например, устанавливается на кабель и пишет все до 60 каналов одновременно на диск. Диск сменный. Снабжена "умным" маяком для ее поиска. Система "Камбала" – для съема информации с подводных кабелей. Шестьдесят магнитофонов по 150 часов записи каждый (всего 9000 часов). В 1981 г. в Охотском море русские сняли такое устройство со своего кабеля.

Зона Е. Радиоэфир. Если радиус действия базовой станции сотовой связи составляет 5…15 км, то перехват сигнала с помощью хорошей аппаратуры можно осуществить на расстоянии до 50км. По этим сигналам можно определить местонахождение абонента, снять и записать информацию. Решается задача "ведения" абонента при его передвижении от одной базовой станции к другой. В мобильной и пейджинговой связи местоположение объекта можно определить даже если разговор не ведется.

3) Несанкционированный съем информации с использованием параллельно расположенных проводников.

Съем информации радиосети, сигнализации и заземления может осуществляться как съем наведенной в параллельном проводнике информации при наличии параллельной прокладки телефонной линии и указанных сетей. Схема съема наведенной информации может выглядеть следующим образом:

Между двумя электрическими цепями (элементами, узлами, средствами), находящимися на некотором расстоянии друг от друга, могут возникать нежелательные электромагнитные связи. Наличие таких связей приводит к тому, что сигналы, циркулирующие в одной цепи (цепи источника наводки), появляются в другой электрической цепи (в цепи рецептора наводки). Основными путями возникновения нежелательных связей являются:

* ближнее электрическое поле;
* ближнее магнитное поле;
* электромагнитное поле излучения;
* соединительные провода, кабели и волноводы, цепи питания, заземления и другие токоведущие элементы и конструкции.

Связь через ближнее электрическое и магнитное поля может рассматриваться как емкостная и индуктивная и смешанная.

Связь через электромагнитное поле. В зону электромагнитных излучений, сопутствующих работе технических средств информационных систем, попадают различные токопроводящие элементы и конструкции, обладающие свойствами антенн (проводники монтажных схем технических средств, токоведущие элементы систем заземления, металлические корпуса аппаратуры, металлоконструкции систем водоснабжения и канализации, провода открытой телефонной или громкоговорящей связи, охранно-пожарной сигнализации, и электропитания и т.д.). Токи опасных сигналов, наводимые электромагнитными полями, сопутствующими работе технических средств, распространяясь по токоведущим коммуникациям, создают реальные предпосылки для утечки информации.

Электромагнитное поле возбуждается в пространстве токами различных радиотехнических устройств (РТУ) или элементов РТУ, не предназначенных для работы в качестве антенны. В зависимости от соотношения между расстоянием r от излучателя до точки приема и длиной волны λ излучаемого поля, пространство вокруг излучателя может быть разделено на три области:

ближняя зона (r << λ);

промежуточная зона (r = λ);

дальняя зона (r >> λ)

Структура и параметры электромагнитных полей, создаваемых токоведущими элементами систем и средств информатизации и связи, определяются их конструктивными особенностями, а также условиями их размещения и эксплуатации. Побочные излучения технических средств обработки информации могут быть в различных участках частотного диапазона.

Телефонные провода и кабели связи так же создают вокруг себя магнитные и электрические поля, образующие каналы утечки информации за счет наводок на другие провода и элементы аппаратуры в ближайшей зоне. Величина наводимой энергии зависит от длины параллельного пробега и расстояния между проводами.

Съем наведенной в параллельном проводнике информации 4) Утечка информации по цепям заземления (преднамеренное соединение объекта с заземляющим устройством).

Защитное заземление, предназначенное для защиты персонала от поражения электрическим током, должно иметь хороший низкоомный контакт с "землей" – наружное заземление.

Рабочее заземление – заземление силового оборудования (сильноточных цепей) и сигнальное или схемное заземление, обеспечивающее формирование опорного потенциала, необходимого для работы электронных схем.

Заземление экранирующих поверхностей (для ослабления нежелательных связей) предназначено для протекания обратных токов в сигнальных цепях и цепях электропитания.

Электромагнитное поле носителя опасного сигнала в местах расположения элементов системы заземления создает в них ток опасного сигнала, попадающий по нулевому проводу в систему заземления и в грунт. Информацию можно снимать как с элементов системы заземления, так и из грунта вокруг заземлителя с помощью дополнительно установленных специальных заземлителей.

5) Утечка информации по цепям питания.

Провода сети питания соединяют различные технические средства и системы, размещенные в различных помещениях, кроме того они являются линейными антеннами, способными излучать или воспринимать электромагнитные поля.

При использовании сети питания как соединяющих проводников чаще всего применяют так называемые сетевые "закладки". К этому типу "закладок" 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. 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.

При использовании сети питания в качестве линейных антенн различают ассиметричные и симметричные наводки.

Ассиметричные наводки имеют место, когда провода сети питания источника и приемника наводки прокладываются вместе и имеют одинаковые емкости относительно источника и приемника наводки. В них наводятся одинаковые по величине и по фазе относительно земли и корпусов приборов напряжения.

Сеть

Эти виды распространения наводок по сети питания являются ассиметричными или однопроводными, поскольку оба провода сети питания передают сигнал наводки в одном направлении. Обратным проводом является земля.

Симметричное распространение наводки имеет место в случае, когда на проводах сети индуцируются различные напряжения относительно земли. Между проводами образуется высокочастотная разность потенциалов, и по проводам сети проходят токи наводки в разных направлениях. В приемнике наводки индуцируются равные по величине и обратные по знаку напряжения, которые не могут проникнуть в высокочастотную часть приемника и не являются опасными.

Вторичные источники питания совместно с подводящими питание линиями могут создавать условия для утечки информации, циркулирующей в питаемом техническом средстве. Колебание амплитуды информационных сигналов приводит к неравномерности потребления тока в цепи питания оконечных каскадов усилителей ТС, что, в свою очередь, приводит к колебаниям напряжения на внутреннем сопротивлении источника вторичного питания.

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