Белорусский государственный университет

Информатики и радиоэлектроники

Кафедра РЭС

Реферат

На тему:

"**Защита информации в телефонных линиях**"

**Минск 2008**

**Защита телефонных каналов.**

При защите телефонных линий как каналов утечки информации необходимо учитывать следующее:

1) телефонные аппараты (даже при положенной трубке) могут быть использованы для перехвата акустической речевой информации из помещений, в которых они установлены, то есть для подслушивания разговоров в этих помещениях;

2) телефонные линии, проходящие через помещения, могут использоваться в качестве источников питания акустических закладок, установленных в этих помещениях, а также для передачи перехваченной информации;

3) возможен перехват (подслушивание) телефонных разговоров путем гальванического или через индукционный датчик подключения к телефонной линии закладок (телефонных ретрансляторов), диктофонов и других средств несанкционированного съема информации.

Телефонный аппарат имеет несколько элементов, способных преобразовывать акустические колебания в электрические сигналы (микрофонный эффект). К ним относятся звонковая цепь, телефонный и, конечно, микрофонный капсюли. За счет электроакустических преобразований в этих элементах возникают информационные (опасные) сигналы. При положенной трубке телефонный и микрофонный капсюли гальванически отключены от телефонной линии и при подключении к ней специальных высокочувствительных низкочастотных усилителей возможен перехват опасных сигналов, возникающих в элементах только звонковой цепи. Амплитуда этих опасных сигналов, как правило, не превышает долей мВ.

При использовании для съема информации метода "высокочастотного навязывания", несмотря на гальваническое отключение микрофона от телефонной линии, сигнал навязывания благодаря высокой частоте проходит в микрофонную цепь и модулируется по амплитуде информационным сигналом. Следовательно, в телефонном аппарате необходимо защищать как звонковую цепь, так и цепь микрофона.

Для недопущения несанкционированного использования ТЛ применяются следующие технические способы (ТС):

* применение пассивных ТС защиты: сигнализаторов подключения, обрыва лини, счетчиков времени разговора, в т.ч. по межгороду;
* применение активных ТС защиты: устройства защиты от параллельного подключения, блокираторы выхода на межгород, устройства кодирования доступа к телефонной линии, устройства активного маскирования информации и др.

**Пассивные ТС защиты телефонной линии.**

К наиболее широко применяемым пассивным методам защиты относятся:

* ограничение опасных сигналов;
* фильтрация опасных сигналов;
* отключение преобразователей (источников) опасных сигналов;

**Ограничения опасных сигналов** основывается на нелинейных свойствах полупроводниковых элементов, главным образом диодов. В схеме ограничителя малых амплитуд используются два встречновключенных диода. Диоды имеют большое сопротивление для токов малой амплитуды и единицы - для токов большой амплитуды (полезных сигналов), что исключает прохождение опасных сигналов малой амплитуды в телефонную линию и практически не оказывает влияние на прохождение через диоды полезных сигналов.

Диодные ограничители включаются последовательно в линию звонка.

Фильтрация опасных сигналов используется главным образом для защиты телефонных аппаратов от "высокочастотного навязывания".

Простейшим фильтром является конденсатор, устанавливаемый в звонковую цепь телефонных аппаратов с электромеханическим звонком и в микрофонную цепь всех аппаратов. Емкость конденсаторов выбирается такой величины, чтобы зашунтировать зондирующие сигналы высокочастотного навязывания и не оказывать существенного влияния на полезные сигналы. Обычно для установки в звонковую цепь используются конденсаторы емкостью 1 мкФ, а для установки в микрофонную цепь - емкостью 0,01 мкФ. Более сложное фильтрующее устройство представляет собой многозвенный фильтр низкой частоты на LC-элементах.

Для защиты телефонных аппаратов, как правило, используются устройства, сочетающие фильтр и ограничитель.

Отключение телефонных аппаратов от линии при ведении в помещении конфиденциальных разговоров является наиболее эффективным методом защиты информации.

Реализация этого метода защиты заключается в установке в телефонной линии специального устройства защиты, автоматически (без участия оператора) отключающего телефонный аппарат от линии при положенной телефонной трубке.

В дежурном режиме (при положенной телефонной трубке) телефонный аппарат отключен от линии, и устройство находится в режиме анализа поднятия телефонной трубки и наличия сигналов вызова. При этом сопротивление развязки между телефонным аппаратом и линией АТС составляет не менее 20 МОм. Напряжение на выходе устройства в дежурном приеме составляет 5...7В. При получении сигналов вызова устройство переходит в режим передачи сигналов вызова, при котором через электронный коммутатор телефонный аппарат подключается к линии. Подключение осуществляется только на время действия сигналов вызова. При поднятии телефонной трубки устройство переходит в рабочий режим и телефонный аппарат подключается к линии. Переход устройства из дежурного в рабочий режим осуществляется при токе в телефонной линии не менее 5 мА. Изделие устанавливается в разрыв телефонной линии, как правило, при выходе ее из выделенного (защищаемого) помещения или в распределительном щитке (кроссе), находящемся в пределах контролируемой зоны.

Контроль состояния телефонной линии и обнаружение атак **осуществляется посредством применения аппаратуры контроля линий связи:**

• индикаторных устройств;

• анализаторов проводных линий и кабельных локаторов (рефлекторметров и устройств, использующих принципы нелинейной локации);

• универсальных комплексов контроля.

Для проведения углубленных исследований телефонных линий на предмет обнаружения несанкционированных подключений подслушивающих устройств используется более серьезная аппаратура, эффективная работа с которой доступна только специалистам. Это анализаторы телефонных линий и кабельные локаторы.

При использовании стандартных анализаторов телефонных линий можно эффективно обнаруживать наличие радиозакладных устройств с непосредственным подключением телефонной линии. Единственное неудобство - необходимость предварительного обесточивания проверяемой линии.

**Телефонный анализатор** в простейшем виде представляет собой комбинацию мультиметра и прибора, позволяющего обнаруживать переделки в телефонном аппарате. С помощью мультиметра отмечаются отклонения от нормальных значений ряда параметров (например, напряжения) абонентской линии связи при снятой и положенной телефонной трубке. Повышенное или пониженное по сравнению со стандартным значением напряжение или сопротивление может означать, соответственно, параллельное или последовательное подключение подслушивающих устройств. Существуют анализаторы, способные инициировать работу РЗУ и тем самым выявлять подслушивающие устройства, приводимые в действие от сигнала вызова уже с помощью детекторов поля или устройств радиоконтроля.

**Рефлектометр (**или «кабельный радар») позволяет определять расстояние до подозрительного места в телефонной линии. Принцип его действия основан на том, что в линию посылается импульс, который отражается от неоднородностей сети, возникающих в местах параллельного и последовательного подключения к ней различных дополнительных устройств. Расстояние до места подключения определяется по положению отраженного импульса на экране электронно-лучевой трубки, зависящему от времени задержки отраженного импульса.

При применении универсальных комплексов контроль осуществляется по изменению уровня сигнала на входе приемника контроля в момент поднятия трубки. Если в линии установлено РЗУ, то процесс поднятия трубки сопровождается существенным изменением уровня принимаемого излучения, кроме того в наушниках прослушивается тональный сигнал номеронабирателя либо другой тестовый сигнал. В «чистой» линии имеет место только кратковременный скачок излучения в момент поднятия трубки (в наушниках слышен короткий щелчок), а тональный набор не прослушивается. Для обеспечения благоприятных условий проверки целесообразно антенну приемника контроля держать как можно ближе к элементам телефонной сети проводу, аппарату, трубке, распределительной коробке и т. д., последовательно перемещая ее от одной точки контроля к другой.

**Аппаратура активной защиты информации в телефонных линиях.**

Активные методы защиты от утечки информации по электроакустическому каналу предусматривают линейное зашумление телефонных линий. Шумовой сигнал подается в линию в режиме, когда телефонный аппарат не используется (трубка положена). При снятии трубки телефонного аппарата подача в линию шумового сигнала прекращается.

К основным методам активной защиты относятся:

* подача во время разговора в телефонную линию синфазного маскирующего низкочастотного сигнала (метод синфазной низкочастотной маскирующей помехи);
* подача во время разговора в телефонную линию маскирующего высокочастотного сигнала звукового диапазона (метод высокочастотной маскирующей помехи);
* подача во время разговора в телефонную линию маскирующего высокочастотного ультразвукового сигнала (метод ультразвуковой маскирующей помехи);
* поднятие напряжения в телефонной линии во время разговора (метод повышения напряжения);
* подача во время разговора в линию напряжения, компенсирующего постоянную составляющую телефонного сигнала (метод "обнуления");
* подача в линию при положенной телефонной трубке маскирующего низкочастотного сигнала (метод низкочастотной маскирующей помехи);
* подача в линию при приеме сообщений маскирующего низкочастотного (речевого диапазона) с известным спектром (компенсационный метод);
* подача в телефонную линию высоковольтных импульсов (метод "выжигания").

Метод синфазной маскирующей низкочастотной (НЧ) помехи заключается в подаче в каждый провод телефонной линии, с использованием единой системы заземления аппаратуры АТС и нулевого провода электросети 220В, согласованных по амплитуде и фазе маскирующих сигналов речевого диапазона частот (300...3400Гц). В телефонном аппарате эти помеховые сигналы компенсируют друг друга и не оказывают мешающего воздействия на полезный сигнал (телефонный разговор). Если же информация снимается с одного провода телефонной линии, то помеховый сигнал не компенсируется. А так как его уровень значительно превосходит полезный сигнал, то перехват информации (выделение полезного сигнала) становится невозможным. В качестве маскирующего помехового сигнала, как правило, используются дискретные сигналы (псевдослучайные последовательности импульсов).

Метод синфазного маскирующего НЧ сигнала используется для подавления телефонных радиозакладок с последовательным (в разрыв одного из проводов) включением, а также телефонных радиозакладок и диктофонов с подключением к линии (к одному из проводов) с помощью индукционных датчиков различного типа.

Метод высокочастотной (ВЧ) маскирующей помехи заключается в подаче во время разговора в телефонную линию широкополосного маскирующего сигнала в диапазоне высших частот звукового диапазона. Данный метод используется для подавления практически всех типов подслушивающих устройств как контактного (параллельного и последовательного) подключения к линии, так и подключения с использованием индукционных датчиков. Однако эффективность подавления средств съема информации с подключением к линии при помощи с индукционных датчиков (особенно не имеющих предусилителей) значительно ниже, чем средств с гальваническим подключением к линии.

В качестве маскирующего сигнала используются широкополосные аналоговые сигналы типа "белого шума" или дискретные сигналы типа псевдослучайной последовательности импульсов. Частоты маскирующих сигналов подбираются таким образом, чтобы после прохождения селективных цепей модулятора закладки или микрофонного усилителя диктофона их уровень оказался достаточным для подавления полезного сигнала (речевого сигнала в телефонной линии во время разговоров абонентов), но в то же время эти сигналы не ухудшали качество телефонных разговоров. Чем ниже частота помехового сигнала, тем выше его эффективность и тем большее мешающее воздействие он оказывает на полезный сигнал. Обычно используются частоты в диапазоне от 6...8 кГц до 16...20 кГц. Такие маскирующие помехи вызывают значительные уменьшение отношения сигнал/шум и искажения полезных сигналов (ухудшение разборчивости речи) при перехвате их всеми типами подслушивающих устройств. Кроме того, у радиозакладок с параметрической стабилизацией частоты ("мягким" каналом) как последовательного, так и параллельного включения наблюдается "уход" несущей частоты, что может привести к потере канала приема.

Для исключения воздействия маскирующего помехового сигнала на телефонный разговор в устройстве защиты устанавливается специальный низкочастотный фильтр с граничной частотой 3,4 кГц, подавляющий (шунтирующий) помеховые сигналы и не оказывающий существенного влияния на прохождение полезных сигналов. Аналогичную роль выполняют полосовые фильтры, установленные на городских АТС, пропускающие сигналы, частоты которых соответствуют стандартному телефонному каналу (300 Гц...3,4 кГц), и подавляющие помеховый сигнал.

Метод ультразвуковой маскирующей помехи в основном аналогичен рассмотренному выше. Отличие состоит в том, что используются помеховые сигналы ультразвукового диапазона с частотами от 20...25 кГц до 50...100 кГц.

Метод повышения напряжения заключается в поднятии напряжения в телефонной линии во время разговора и используется для ухудшения качества функционирования телефонных радиозакладок. Поднятие напряжения в линии до 18...24В вызывает у радиозакладок с последовательным подключением и параметрической стабилизацией частоты "уход" несущей частоты и ухудшение разборчивости речи вследствие размытия спектра сигнала. У радиозакладок с последовательным подключением и кварцевой стабилизацией частоты наблюдается уменьшение отношения сигнал/шум на 3...10 дБ. Телефонные радиозакладки с параллельным подключением при таких напряжениях в ряде случаев просто отключаются.

Метод "обнуления" предусматривает подачу во время разговора в линию постоянного напряжения, соответствующего напряжению в линии при поднятой телефонной трубке, но обратной полярности.

Этот метод используется для нарушения функционирования подслушивающих устройств с контактным параллельным подключением к линии и использующих ее в качестве источника питания. К таким устройствам относятся: параллельные телефонные аппараты, проводные микрофонные системы с электретными микрофонами, использующие телефонную линию для передачи информации, акустические и телефонные закладки с питанием от телефонной линии и т.д.

##### **Метод низкочастотной маскирующей помехи** заключается в подаче в линию при положенной телефонной трубке маскирующего сигнала речевого диапазона частот (300...3400Гц). Применяется для подавления проводных микрофонных систем, использующих телефонную линию для передачи информации на низкой частоте, а также для активизации (включения на запись) диктофонов, подключаемых к телефонной линии с помощью адаптеров или индукционных датчиков, что приводит к сматыванию пленки в режиме записи шума (т.е. при отсутствии полезного сигнала).

Компенсационный метод используется для односторонней маскировки (скрытия) речевых сообщений, передаваемых абоненту по телефонной линии.

Суть метода заключается в следующем. При передаче скрываемого сообщения на приемной стороне в телефонную линию при помощи специального генератора подается маскирующая помеха (цифровой или аналоговый маскирующий сигнал речевого диапазона с известным спектром). Одновременно этот же маскирующий сигнал ("чистый" шум) подается на один из; входов двухканального адаптивного фильтра, на другой вход которого поступает аддитивная смесь принимаемого полезного сигнала речевого сигнала (передаваемого сообщения) и этого же помехового сигнала. Аддитивный фильтр компенсирует (подавляет) шумовую составляющую и выделяет полезный сигнал, который подается на телефонный аппарат или устройство звукозаписи.

Недостатком данного метода является то, что маскировка речевых сообщений односторонняя и не позволяет вести двухсторонние телефонные разговоры.

Метод "выжигания" реализуется путем подачи в линию высоковольтных (напряжением более 1500 В) импульсов, приводящих к электрическому "выжиганию" входных каскадов электронных устройств перехвата информации и блоков их питания, гальванически подключенных к телефонной линии.

При использовании данного метода телефонный аппарат от линии отключается. Подача импульсов в линию осуществляется два раза. Первый раз - для "выжигания" параллельно подключенных устройств при разомкнутой телефонной линии, второй раз - для "выжигания" последовательно подключенных устройств при закороченной (как правило, в центральном распределительном щитке здания) телефонной линии.

Современные контроллеры телефонных линий, как правило, наряду со средствами обнаружения подключения к линии устройств несанкционированного съема информации, оборудованы и средствами их подавления. Для подавления в основном используется метод высокочастотной маскирующей помехи. Режим подавления включается автоматически или оператором при обнаружении факта несанкционированного подключения к линии.

**Защита речевой информации в IP-телефонии.**

В IP-телефонии существуют два основных способа передачи пакетов с речевой информацией по сети: через сеть Интернет и через корпоративные сети + выделенные каналы. Между этими способами мало различий, однако во втором случае гарантируется лучшее качество звука и небольшая фиксированная задержка пакетов речевой информации при их передаче по IP-сети.

Для защиты речевой информации, передаваемой в IP-сетях, применяются криптографические алгоритмы шифрования исходных пакетов и сообщений, которые позволяют обеспечить гарантированную устойчивость IP-телефонии. Существуют эффективные реализованные на ПЭВМ криптографические алгоритмы, которые при использовании 256-битных секретных и 1024-битных открытых ключей шифрования (например, по ГОСТ 28147-89) практически делают невозможным дешифрование речевого пакета. Однако при использовании в IP-телефонии таких алгоритмов следует учитывать несколько важных факторов, которые могут свести на нет возможности многих современных средств криптографической защиты информации.

Для обеспечения приемлемого качества звука на приемной стороне при передаче речевых пакетов в IP-сети задержка в их доставке от приемной стороны не должна превышать 250 мс. Для уменьшения задержки оцифрованный речевой сигнал сжимают, а затем зашифровывают с использованием алгоритмов потокового шифрования и протоколов передачи в IP-сети.

Другой проблемой защищенной IP-телефонии является обмен криптографическими ключами шифрования между абонентами сети. Как правило, используются криптографические протоколы с открытым ключом с применением протокола Диффи-Хеллмана, который не дает тому, кто перехватывает разговор, получить какую-либо полезную информацию о ключах и в то же время позволяет сторонам обменяться информацией для формирования общего сеансового ключа. Этот ключ применяется для зашифровки и расшифровки речевого потока. Для того, чтобы свести к минимуму возможность перехвата ключей шифрования, используются различные технологии аутентификации абонентов и ключей.

Все криптографические протоколы и протокол сжатия речевого потока выбираются программами IP-телефонии динамически и незаметно для пользователя, предоставляя ему естественный интерфейс, подобный обычному телефону.

Реализация эффективных криптографических алгоритмов и обеспечение качества звука требуют значительных вычислительных ресурсов. В большинстве случаев эти требования выполняются при использовании достаточно мощных и производительных компьютеров, которые, как правило, не умещаются в корпусе телефонного аппарата. Но межкомпьютерный обмен речевой информацией не всегда устраивает пользователей IP-телефонии. Гораздо удобнее использовать небольшой, а лучше мобильный аппарат IP-телефонии. Такие аппараты уже появились, хотя они обеспечивают стойкость шифрования речевого потока значительно ниже, чем компьютерные системы IP-телефонии. В таких телефонных аппаратах для сжатия речевого сигнала используется алгоритм GSM, а шифрование осуществляется по протоколу Wireless Transport Layer Security (WTLS), который является частью протокола Wireless Application Protocol (WAP), реализованного в сетях мобильной связи. По прогнозам экспертов, будущее именно за такими телефонными аппаратами: небольшими, мобильными, надежными, имеющими гарантированную стойкость защиты речевой информации и высокое качество звука

**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.