Проблемы безопасности телефонных сетей общего пользования

Введение

В наши дни информация может иметь слишком большую ценность, чтобы можно было спокойно смотреть на ее возможную утечку (по данным США вероятность утечки информации по телефонной линии составляет 5 - 20%). Поэтому не последнее место наряду со множеством мероприятий, проводимых по защите информации, занимает организация защиты телефонных линий связи. Любому должностному лицу в работе необходим телефон, в то время как сведения, которые можно получить по телефонной линии позволяют определить профиль работ, возможных партнеров, а также другую ценную информацию, что является недопустимым в условиях нашего «дикого» рынка. Ведь в случае полного рассекречивания информации о деятельности коммерческой фирмы, последняя , по мнению экспертов, просуществует от нескольких часов до нескольких дней. Следовательно, закрытие телефонной линии связи также необходимо, как и любое другое мероприятие по защите информации, и должно носить комплексный характер и соответствовать ценности охраняемой информации.

Возможные каналы утечки информации

При организации защиты телефонных линий связи следует учитывать:

1. Возможность прослушивания помещений, в которых установлены телефонные аппараты;
2. Возможность использования телефонных линий в качестве источников питания для электронных устройств перехвата акустической информации, а также передачи перехваченной информации;
3. Возможность перехвата информации специальными электронными устройствами путем гальванического подключения к телефонной линии;
4. Возможность несанкционированного использования телефонной линии в корыстных целях.

Методы съема и защиты информации при разговорах, ведущихся в помещении, через телефон.

Элементы телефонного аппарата (такие как звонковая цепь, микрофонный и телефонный капсюли и др.) могут преобразовывать колебания из акустических в электрические, что позволяет прослушивать разговоры в помещениях, где они установлены.

При положенной телефонной трубке информационные сигналы возникают в элементах только звонковой цепи, т.к. телефонный и микрофонный капсюли гальванически отключены от телефонной линии. Перехват этих сигналов возможен путем гальванического подключения к телефонной линии специальных высокочувствительных низкочастотных усилителей. Однако дальность перехвата информации в данном случае (вследствие малой амплитуды сигналов) не превышает нескольких десятков метров.

Первый способ увеличения дальности перехвата состоит в подключении к телефонной линии низкочастотного усилителя через устройство анализа состояния, которое при положенной трубке отключает линию от АТС и подключает усилитель, а при поднятии трубки или звонке производит обратные действий. Вследствие уменьшения уровня шумов в линии за счет отключения телефонного аппарата от АТС в момент съема информации повышается дальность перехвата.

Второй способ заключается в использовании метода «высокочастотного навязывания», осуществляемого путем контактного введения токов высокой частоты от генератора, подключенного к телефонной линии. Благодаря высокой частоте (от 30 кГц до 10 МГц и более) сигнал «навязывания» проходит и в звонковую, и в микрофонную цепи. Далее высокочастотный сигнал, промодулированный речевым, отражается от несогласованной нагрузки (т.е. нелинейных или параметрических элементов телефонного аппарата) и распространяется в обратном направлении по линии. Там он принимается и обрабатывается специальным приемным устройством, также подключаемым к телефонной линии. Дальность перехвата информации при использовании данного метода увеличивается до нескольких сот метров.

Для прослушивания разговоров в помещениях помимо электрических каналов утечки информации могут применяться электронные устройства перехвата речевой информации, использующие телефонную линию для передачи информации как на низких (в речевом диапазоне), так и на высоких частотах (от 40 кГц до 10 МГц и более). В случае низких частот для передачи информации используются микрофонные проводные системы и устройства типа «телефонное ухо». Последние включают в себя микрофон, микрофонный усилитель, электронный коммутатор и устройство анализа состояния телефонной линии. В качестве приемника может быть использован низкочастотный усилитель или такие устройства записи речевой информации как магнитофон и диктофон, подключаемые к линии с помощью специального адаптера. Дальность передачи информации в этом случае может составлять несколько километров.

Существуют активные и пассивные методы и средства защиты телефонного аппарата от утечки речевой информации по электроакустическому каналу и от перехвата электронными устройствами. К наиболее рапространенным пассивным методам защиты относятся:

- ограничение опасных сигналов;
- фильтрация опасных сигналов;
- отключение источников опасных сигналов.

Благодаря нелинейным свойствам полупроводниковых элементов (в первую очередь диодов) существует возможность ограничения опасных сигналов. В схеме ограничителя малых амплитуд используются два встречновключенных диода, которые образуют зону нечувствительности для микро ЭДС. Это объясняется разницей внутреннего сопротивления диода для токов малой амплитуды (сотни кОм) и большой (единицы Ом и менее) в интервале 0-0.65В. Т.о. исключается прохождение в телефонную линию опасных сигналов малой амплитуды при свободном «прохождении» звукового сигнала абонента и напряжения вызова.

Фильтрация опасных сигналов в основном используется для защиты от «высокочастотного навязывания». Конденсатор является простейшим фильтром и устанавливается в микрофонную цепь (емкость 0,01-0,05 мкФ) и в звонковую цепь телефонных аппаратов с электромеханическим звонком (емкость 1 мкФ). Более сложным устройством фильтрации является многозвенный фильтр низкой частоты на LC – элементах. В наши дни в основном используются комплексные схемы, включающие и фильтр, и ограничитель.

Наиболее эффективным методом защиты информации является отключение телефонных аппаратов от линии при ведении конфиденциальных разговоров в помещении, где они установлены. Простейший способ реализации этого метода состоит в установке в корпусе телефонного аппарата или телефонной линии специального выключателя, при положенной телефонной трубке отключающего телефонный аппарат от линии либо вручную, либо автоматически.

Активные методы защиты от утечки информации по электроакустическому каналу сводятся к методу низкочастотной маскирующей помехи, который состоит в подаче в телефонную линию (при положенной трубке) маскирующего низкочастотного (от 100Гц до 10кГц) шумового сигнала. Для защиты информации от перехвата электронными устройствами существует еще один метод (метод высокочастотной широкополосной маскирующей помехи), который заключается в подаче в телефонную линию при положенной телефонной трубке маскирующего высокочастотного (от 20кГц до 30МГц) широкополосного шумового сигнала.

Методы съема и защиты информации при прослушивании телефонных разговоров.

Прослушивание телефонных разговоров возможно благодаря электронным устройствам перехвата речевой информации, подключаемым к телефонным линиям одним из трех способов: последовательно (в разрыв одного из проводов), параллельно (одновременно к двум проводам) и с использованием индукционного датчика (бесконтактное подключение). В случае первых двух подключений питание электронных устройств перехвата осуществляется от телефонной линии, при последнем - от автономного источника тока. Активизация радиопередающего устройства происходит только на время телефонного разговора, при этом может осуществляться запись получаемой речевой информации. Также возможно прослушивание через подключение второго телефонного аппарата в соседней комнате.

Существует несколько активных методов для защиты телефонных разговоров, осуществляющих подавление электронных устройств перехвата информации, основные из которых описаны ниже.

Метод высокочастотной маскирующей помехи заключается в подаче в линию во время телефонного разговора широкополосного маскирующего помехового сигнала, частота которого подбирается так, чтобы после прохождения микрофонного усилителя диктофона его уровень оказался достаточным для подавления речевого сигнала, но при этом не ухудшалось качество телефонных разговоров. Эффективность помехового сигнала повышается с понижением его частоты, т.е. чем ниже

его частота, тем большее мешающее воздействие он оказывает на полезный (речевой) сигнал. Обычно используются сигналы с частотой в диапазоне от 6-8 до 16-20 кГц. Также для исключения воздействия маскирующего помехового сигнала на качество связи в устройстве защиты устанавливается специальный низкочастотный фильтр с граничной частотой выше 3,4 кГц, выполняющий ту же роль, что и полосовые фильтры на городских АТС, пропускающие сигналы с частотой, соответствующей стандартному телефонному каналу, и подавляющие помеховый сигнал. Данный метод пригоден для подавления большинства типов электронных устройств перехвата речевой информации всех видов подключения к телефонной линии.

Метод «ультразвуковой» маскирующей помехи отличается от предыдущего тем, что используемые частоты помехового сигнала находятся в диапазоне от 20-25 до 50-100 кГц.

Метод «обнуления» заключается в том, что в момент телефонного разговора в линию подается постоянное напряжение, которое с обратной полярностью соответствует напряжению в линии при поднятой телефонной трубке. Данный метод применим для вывода из строя электронных устройств перехвата речевой информации с контактным подключением к телефонной линии, использующих ее для питания. К подобным устройствам можно отнести параллельные телефонные аппараты и телефонные радиозакладки.

Метод низкочастотной маскирующей помехи аналогичен методу высокочастотной маскирующей помехи, описанному ранее. Методы отличаются частотой маскирующих помех, а также случаями использования. Рассматриваемый метод (метод низкочастотной маскирующей помехи) применяется для несвоевременной активации диктофонов и других записывающих устройств, подключенных к телефонной линии через адаптеры или индукционные датчики, в результате которой происходит сматывание пленки в режиме записи шума (т.е. при отсутствии полезного (речевого) сигнала).

Компенсационный метод заключается в том, что при передаче речевого сообщения на принимающей стороне с помощью специального генератора в телефонную линию и на один из входов двухканального адаптивного фильтра подается маскирующая помеха, на другой вход фильтра поступает адаптивная смесь принимаемого полезного (речевого) и того же помехового сигналов. Далее адаптивный фильтр выделяет полезный сигнал путем компенсации шумовой состовляющей и посылает его на телефонный аппарат или записывающее устройство. Этот метод является высокоэффективным для подавления всех известных средств несанкционированного съема информации с телефонной линии и широко используется для маскировки, а также сокрытия речевых сообщений передаваемых абонентом.

Метод «выжигания» заключается в подаче в телефонную линию высоковольтных импульсов напряжением более 1500В, в результате чего входные каскады электронных устройств передачи информации и блоки их питания, гальванически подключенные к телефонной линии,

претерпевают электрическое «выжигание». Телефонный аппарат в случае использования этого метода от линии отключается. Импульсы подаются в телефонную линию дважды. Один раз при разомкнутой телефонной линии (для «выжигания» паралельно подключенных к ней электронных устройств), а второй - при закороченной (для "выжигания" последовательно подключенных устройств). Телефонный аппарат в случае использования этого метода от линии отключается.

В настоящее время для защиты телефонных линий используются не только простые устройства, реализующие один из методов защиты, но и сложные, которые обеспечивают комплексную защиту линий путем комбинации нескольких методов, включающих защиту информации от утечки по электроакустическому каналу.

Защита от несанкционированного использования телефонной линии.

Отдельной, но очень актуальной проблемой является борьба с несанкционированным использованием телефонной линии в корыстных целях, таких как дорогостоящие междугородние и международные звонки. Проблема обострилась с массовым распространением всевозможных видов радиотелефонов.

Технические способы защиты можно традиционно разбить на две основные группы:

- пассивные;
- активные.

Пассивные устройства защиты существуют лишь для регистрации факта несанкционированного подключения и самовольного использования линии, в то время как активные устройства защиты предусматривают вмешательство в эти процессы.

Сейчас наряду с несанкционированными подключениями на участках проводной связи возрастает количество «пиратских» подключений в зоне радиоканала. В тоже время службы АТС не способны решить данную проблему на радиочастоте.

В первых моделях «российских» радиотелефонов использовалось два способа защиты от «пиратства»: скачкообразное изменение частоты и наличие индивидуального номера у каждой трубки, зарегистрированной на базе аппарата, без которого невозможно опознание. Однако это не надолго решило проблему, т.к. на «черном» рынке скоро появились так называемые «трубки-сканеры», с помощью которых возможно отслеживание скачкообразного изменения частоты (тем более, что количество фиксированных частот работы очень ограничено) и подбор индивидуального номер трубки методом перебора.

Единственным эффективным способом борьбы без изменения принципиальной схемы радиотелефона является установка блокиратора межгорода и блока дополнительного кодирования линии. Существует также радикальный способ решения этой непростой ситуации - появление радиотелефонов, отвечающих стандарту DECT, похожего по принципу построения используемоего в сотовой связи GSM.

Литература:

1. Андрианов В.И. и др. - Шпионские штучки и устройства для защиты объектов и информации: справочное пособие. СПб.: «Лань», 1996.
2. Баранов В.М. Вальков Г.В., Еремеев М.А. и др. Защита информации в системах и средствах связи. Учебное пособие. С-Пб: ВИККА им. А.Ф.Можайского, 1994.
3. Каторин Ю.Ф., КуренковЕ.В., Лысов А.В. и др. Энциклопедия промышленного шпионажа / Антишпионские штучки / С-Пб.: ООО «Полигон», 2000.
4. Лагутин В.С., Петраков А.В. Утечка и защита информации в телефонных каналах. М.: Энергоатомиздат, 1996.
5. Торокин А.А. Основы инженерно-технической защиты информации. М.: «Ось», 1998.
6. Хореев А. А. Защита информации от утечки по техническим каналам. Ч1. Технические каналы утечки информации. М: Гостехкомиссия, 1998.
7. Хореев А. А. Способы и средства защиты информации. Учебное пособие. М.: МО РФ, 2000.