УДК 007.681

Булкин В.А.

ТЕХНОЛОГИЯ ЗАЩИТЫ ТЕЛЕФОННЫХ РАЗГОВОРОВ

Телефонные угрозы и степень их опасности. Контроль телефонных разговоров остается одним из наиболее распространенных видов промышленного шпионажа и действий преступных элементов. Причины очевидны – малые затраты и риск реализации угроз, необязательность захода в контролируемое помещение, разнообразие способов и мест съема информации и пр.

Контролировать телефонные разговоры можно на всем протяжении телефонной линии, а при использовании сотовой-телефонной связи – во всей сотовой зоне.

Средства перехвата, предлагаемые на российском рынке, реализуют различные физические принципы и современные программно-аппаратные решения. В их числе: разнообразные устройства контактного и бесконтактного подключения к телефонным линиям; специальные телефонные "жучки" и ответчики; комплексы перехвата сотовой связи во всех ее стандартах и пр.

Основой любой системы защиты информации, любого плана противодействий является знание угроз и степени их опасности.

Формально степени опасности угроз отражают вероятности их реализации за некоторое условное время. Совокупную опасность характеризует спектр угроз, представляющий собой их перечисление в порядке уменьшения степени опасности.

Авторская версия спектра "телефонных" угроз, основанная на их экономико-статистической модели, представлена на рис. 1. Там же дана расшифровка использованных символьных обозначений.

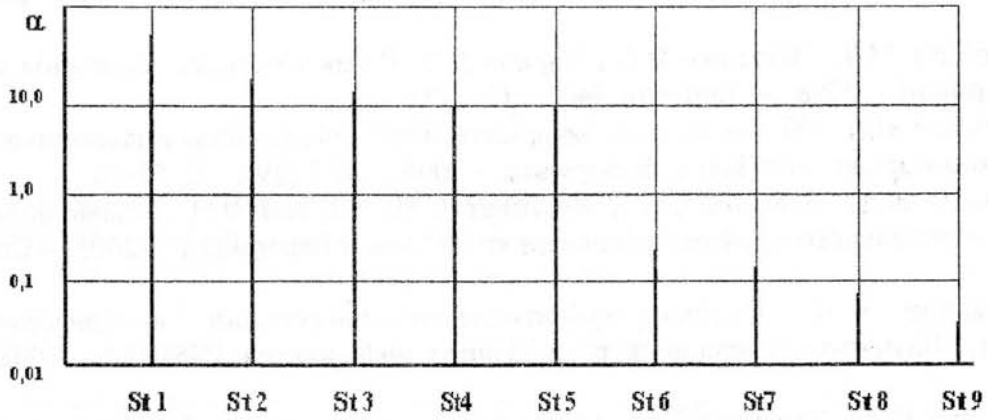

Рис. 1. Спектр «телефонных» угроз

St1 - простейшее контактное подключение к линии
St2 - применение телефонного "жучка"
St3 - индукционное подключение к линии
St4 - профессиональное подключение к линии (фильтрация внеполосных помех)
St5 - емкостное подключение к линии
St6 - перехват радиотелефона в стандарте AMPS(DAMPS)
St7 - перехват радиотелефона в стандарте NMT
St8 - перехват радиотелефона в стандарте GSM
St9 - перехват спутниковой телефонной связи (в ближней зоне)

Спектр угроз показывает нам, что:

- наибольшую опасность представляет собой контроль телефонных разговоров с помощью простейшего контактного подключения к линии.
- примерно равную, но меньшую опасность представляет перехват телефонных разговоров с проводных линий с помощью "жучков", ответчиков и бесконтактного съема информации
- существенно меньшую (почти на порядок) опасность представляют собой угрозы, связанные с перехватом сотовой телефонной связи, особенно в стандарте GSM.
- минимальная опасность прогнозируется для спутниковой телефонной связи.

"Телефонная безопасность" и способы ее обеспечения. Современные средства и методы защиты телефонных разговоров от перехвата отражают множественность угроз и разнообразие сценариев их реализации. Различия проявляются прежде всего в тактических особенностях.

Укрупнено можно выделить две основных тактических разновидности противодействий:

- средства физической защиты информации, включающие в себя постановщики заградительных помех, нейтрализаторы, фильтры и средства физического поиска каналов утечки информации;
- средства смысловой (в частности, криптографической) защиты информации.

Краткий комментарий к ним сводится к следующему:

Подавляющее большинство постановщиков заградительных помех предназначено для использования с проводными линиями телефонной связи (в основном для защиты участка "телефонный аппарат – АТС"). Помеха создается, как правило, **вне полосы** речевого сигнала и превышает его номинальный уровень на один – два и более порядков.

Наличие интенсивной помехи выводит из линейного режима все простейшие устройства контактного и бесконтактного подключения к телефонной линии (появляется шум в звуковом диапазоне, происходит подавление сигнала в канале перехвата). В самом телефонном аппарате абонента зашумление не ощущается благодаря предварительной пассивной высокочастотной фильтрации входного сигнала.

В отличие от постановщиков заградительных помех нейтрализаторы предназначены для создания необратимых и реже обратимых изменений (нарушений) работоспособности устройств контактного несанкционированного подключения к телефонной линии. С этой целью с их помощью на линии создается кратковременное высоковольтное (около 1500 вольт) напряжение, "прожигающее" подключаемые устройства.

Для исключения угроз, связанных с использованием микротоков и высокочастотных "навязываний" применяют специальные фильтры и блокираторы телефонных аппаратов.

Современная номенклатура средств физического поиска каналов перехвата телефонных разговоров включает в себя:

- аппаратные и программно-аппаратные средства радиомониторинга, позволяющие эффективно выявлять телефонные "жучки". К ним, в частности, относятся сравнительно недорогие индикаторы поля и более дорогие сканеры;
- технические средства выявления изменений активных и реактивных импедансов телефонных линий, возникающих при появлении дополнительной нагрузки. В простейшем случае это – телефонные проверочные устройства, выявляющие резистивные изменения и изменения напряжения в телефонной сети. В более сложных вариантах это – анализаторы телефонных линий, позволяющие выявлять бесконтактные несанкционированные подключения.

Криптографическая защита телефонных разговоров рассматривается специалистами как единственная пока возможность гарантированной защиты телефонных каналов связи от

перехвата независимо от того, ведутся ли они по проводным или беспроводным линиям связи. *(Следует отметить, что отказ от привычного аналогового способа передачи сообщений и переход к цифровой передаче информации повышает защищенность телефонных каналов даже при отсутствии кодирования.)*

Соответствующие устройства получили название скремблеров.

Анализ современных средств защиты телефонных каналов связи, основанный на ранговой сравнительной метрологии, показывает, что:

- наибольший приоритет имеют постановщики заградительных помех в телефонных линиях, телефонные проверочные устройства и анализаторы линий, индикаторы радиополей (как инструменты выявления телефонных "жучков")
- криптографические средства защиты информации в проводных и беспроводных каналах телефонной связи имеют сравнительно небольшие ранговые коэффициенты из-за необходимости одновременного оснащения скремблерами достаточно большого числа абонентов. Область их экономически рационального использования – закрытые сети служебной телефонной связи.

От анализа рынка к новой технологии защиты. Выявленный приоритет постановщиков заградительных помех определил необходимость не только параметрического их совершенствования, но и целесообразность ревизии данного вида противодействий в целом складывалась примерно следующая схема рассуждений.

Прежде всего, необходимо заменить "внеполосную" заградительную помеху, действующую за границей спектра частот, на "полосную", которая будет действовать непосредственно в диапазоне частот речевых сообщений. Это- условие полной гарантии защиты телефонных разговоров от перехвата на тех участках линии, где помеха существенно превышает уровень информационного речевого сигнала.

Далее. Очевидно, что создаваемую помеху сможет скомпенсировать только тот, кто ее создает, т.е. подобная маскировка телефонных сообщений принципиально односторонняя.

Значит необходимо отказаться от привычной схемы обязательной защиты "входящих" и "исходящих" телефонных.

Складывается следующая цель рассуждений принципиального характера.

Прежде всего, необходимо заменить " внеполосную" заградительную помеху, действующую за границей спектра речевых частот, на "полосную", которая будет действовать непосредственно в спектре частот речевых сообщений. Это условие даст нам полную гарантию защиты телефонных разговоров от перехвата на тех участках линии, где помеха существенно превышает уровень информационного речевого сигнала.

Далее. Очевидно, что создаваемую "полосную" помеху сможет скомпрометировать только, тот, кто ее создает, т.е. подробная маскировка телефонных сообщений принципиально односторонняя.

Значит необходимо отказаться от привычной схемы обязательной защиты телефонных сообщений в течение всей их продолжительности, и перейти к новой технологии, при которой защищается только "входящая" информация в моменты времени , соответствующие ее значимости.

Технологию защиты поясняет схема на рис. 2. Абонент №1, имеющий односторонний маскиратор, получает входной звонок от некоторого абонента №2, не имеющего в общем случае такого маскиратора *(При наличии у него маскиратора связь становится с двухсторонней защитой)* "Входящий" звонок может быть с любого городского (междугороднего) телефона, включая таксофон и радиотелефон сотовой связи. В момент передачи важных сообщений, требующих защиты (о чем абонент №2 извещает открытым текстом), абонент №1 подключает к линии маскиратор речи, создающий в линии достаточно интенсивный шум. Этот шум слышит абонент №2, но продолжает разговор, не меняя голоса.

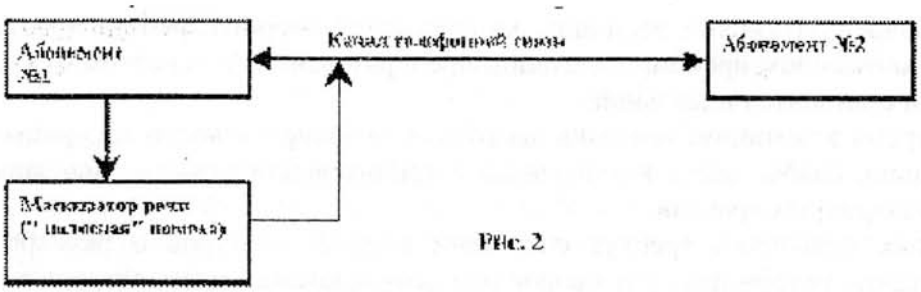

Рис. 2

В отличие от него абонент №1 шума не слышит, он воспринимает "чистую" речь, поскольку шум при приеме автоматически компенсируется. По завершении приема важных сведений заградительная помеха отключается.

Уровень вносимого в линию шума ограничен только возникающими нелинейными искажениями. Но, как показали исследования, этот предел не препятствует защите смыслового содержания и даже защите признаков речи (на приемном конце).

Принцип действия одностороннего маскиратора. Инструментальной основой маскираторов речи "Туман" являются современные двухканальные цифровые адаптивные фильтры представлена структурная схема маскиратора

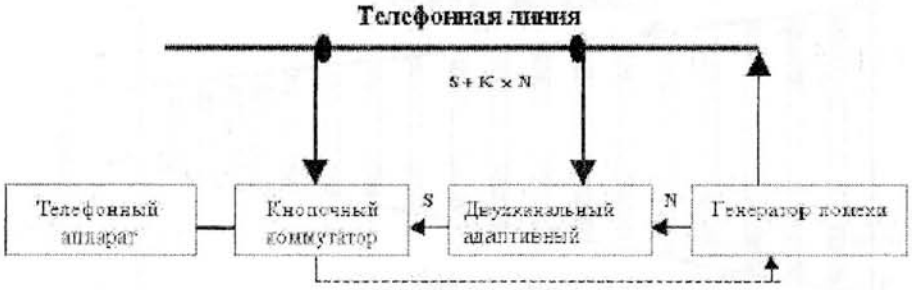

Рис. 3

Основных функциональных блока три:

- генератор маскирующей помехи (цифровой или аналоговый)
- двухканальный адаптивный фильтр
- кнопочный коммутатор (для управления режимом работы)

Выполняемая адаптивным фильтром функция сводится к компенсации помехи, создаваемой в линии генератором. С этой целью на один из входов фильтра подается "чистый" шум с известным спектром N(jw), а на другой – аддитивная смесь принимаемого (полезного) речевого сигнала S(jw) и той же помехи , но с измененной в общем случае (вследствие прохождения через телефонный тракт) спектральной характеристикой N(jw)*K(jw), где K(jw) – неизвестный заранее комплексный коэффициент передачи телефонного тракта.

Адаптивный фильтр анализирует сигналы, поступающие на его входы, и подбирает некоторое спектральное преобразование A(jw) над "чистым" шумом такое, чтобы обеспечивалось максимальное подавление шума в разности принимаемой по одному из входов смеси Y(jw)=S(jw)+N(jw)*K(jw) полезного сигнала с помехой и преобразованной помехи N(jw)*A(jw).

Минимальные средне-квадратические ошибки фильтрации имеют место при

$$A(jw) = \{Y(jw)*N(jw)\}/\{N^2(jw)\},$$

где символ {z} - означает усреднение величины z в течение некоторого времени адаптации.

При достаточно большом времени адаптации преобразование A(jw) стремится к K(jw), компенсация помехи становится идеальной.

Чем меньше время адаптации, тем, вообще говоря, меньше точность воспроизведения K(jw) и, следовательно, слабее ведет компенсация заградительной помехи. Все зависит от реальных свойств телефонных трактов.

Дополнительных пояснений требует еще один вопрос – вопрос о размерах зоны гарантированной защиты телефонных разговоров при использовании маскираторов речи.

Если бы телефонные линии были идеальны (т.е. не вносили затухание "входящих" и "исходящих" сигналов), то степень маскировки, оцениваемая спектральным отношением шум/сигнал N(jw)/S(jw) была бы одинаковой по всей протяженности проводной телефонной линии.

В действительности реальные телефонные линии вносят затухание сигналов. Величина его в городских условиях может достигать 20 и более дБ.

Наличие затухания уменьшает спектральное отношение помеха/сигнал при движении в сторону "входящего" телефонного сообщения. На рис. 4 представлена условная диаграмма уровней помехи и "входящего" сигнала для случая, когда отсутствует промежуточное их усиление.

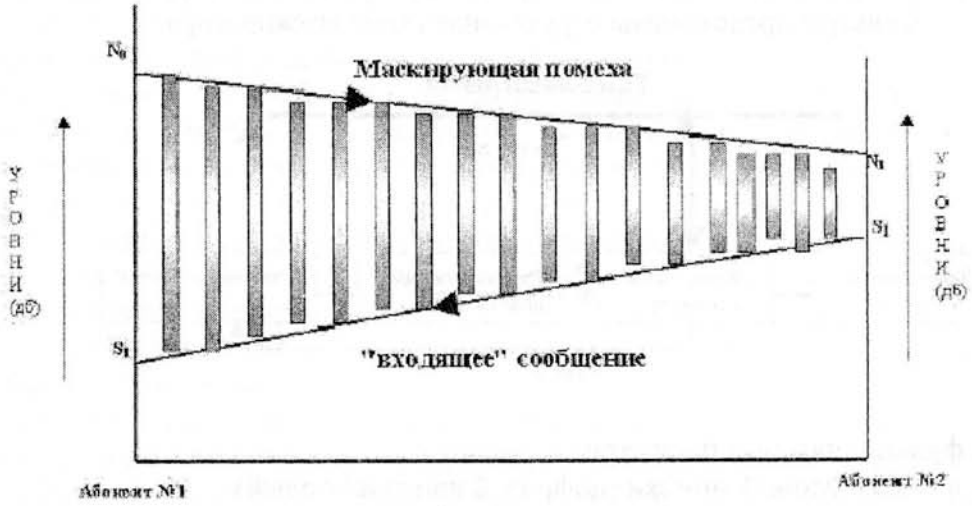

Рис. 4

Из диаграммы, в частности, следует, что отношение помеха/сигнал (или разность их уровней в децибелах) меняется от своего максимального значения $N_0 - S_1$ до минимальной величины $N_1 - S_0$ у источника "входящего" сообщения.

Реальное затухание в городской телефонной линии на участке абонент-АТС не превышает 10 дБ. В этих условиях "входящее" речевое сообщение будет закрыто помехой на всем рассматриваемом участке. Минимальная маскировка $N_1 - S_0$ будет в районе АТС, ее уровень оценивается величиной не менее 10 дБ.

От частного к общему. Односторонняя маскировка шумом "входящих" сообщений, рассмотренная нами как новая технология защиты телефонных разговоров от перехвата, может иметь более широкое практическое применение в индустрии информационной безопасности.

Одно из возможных применений – закрытая передача паролей, ключей, идентификационных и аутентификационных признаков впо каналам компьютерной связи.

В качестве примера представим себе ситуацию, когда необходимо передать по компьютерной сети важную информацию. Гарантию ее защиты можно дать только при использовании криптографических методов, но в данном случае не было передачи закрытых

ключей. Ситуация не совсем гипотетическая.

Предположим теперь, что получатель информации располагает некоторым программно-аппаратным средством, позволяющим ему временно закрыть канал связи цифровым шумом и компенсировать его при приеме. Он извещает владельца информации о своей готовности и зашумляет канал связи.

Владелец информации осуществляет передачу ключей по зашумленному каналу. По завершении передачи ключей шум выключается и осуществляется передача информации обычным способом по схеме закрытого ключа.

При наличии подобных устройств с обоих концов обмен ключевой информацией может осуществляться двусторонне, причем автоматически.

Реализуется, таким образом, идея криптографической защиты информации с одноразовыми закрытыми ключами. Это – новая и вполне реальная технология.

Список литературы

1.Баранов В.М., Вальков Г.В., Еремеев М.А. и др. Защита информации в системах и средствах связи. Учебное пособие.– Санкт- Петербург: ВИККА имени А.Ф. Можайского. 2007.

2.Лагутин В.С., Петраков А.В. Утечка и защита информации в телефонных каналах.– М.: Энергоатомиздат. 2008.

3.Устройство защиты телефонных линий и помещений от прослушивания 2008.

Поступила 07.01.2009

УДК 003.26:621.39+530.145 **Василиу Е.В., Николаенко С.В.**

БЕЗОПАСНАЯ СИСТЕМА ПРЯМОЙ ПЕРЕДАЧИ СООБЩЕНИЙ НА ОСНОВЕ ПИНГ – ПОНГ ПРОТОКОЛА КВАНТОВОЙ БЕЗОПАСНОЙ СВЯЗИ

Введение

В информационном обществе все большее количество людей испытывают необходимость в конфиденциальной связи. Квантовые коммуникации, основанные на передаче информации, закодированной в отдельных квантовых состояниях, предлагают ряд новых способов для безопасного обмена сообщениями. Например, квантовые протоколы распределения ключей служат для создания секретного ключа, используя который две авторизованные стороны, Алиса и Боб, могут затем обмениваться секретными сообщениями с использованием алгоритмов классической криптографии [1]. Другое направление квантовых коммуникаций – квантовые протоколы безопасной связи (КПБС), в которых секретный ключ вообще не используется, а его роль в некотором смысле играет информационный ресурс квантовой механики – совместно используемые авторизованными пользователями группы перепутанных квантовых частиц [2 – 9]. Секретное сообщение, закодированное с помощью квантовых состояний таких групп кубитов, передается непосредственно через квантовый канал связи (в качестве таких каналов можно использовать существующие оптические каналы). При этом законы квантовой механики гарантируют обнаружение подслушивание в канале, для чего легитимные стороны должны выполнить определенную последовательность квантовых измерений над некоторой частью переданных кубитов. Обнаружив подслушивающего агента, Еву, Алиса и Боб прекращают передачу сообщения.