МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

DOI 10.17223/20710410/2/14

УДК 681.3

МЕТОДЫ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ

А.М. Гришин

Институт криптографии, связи и информатики Академии ФСБ России, г. Москва

E-mail: av123470@comtv.ru

В статье рассматриваются основные задачи, которые возникают при построении системы защиты речевых сигналов, и даются рекомендации по их решению.

Ключевые слова: *защита речи, криптографические методы защиты.*

Человеческая речь, и в частности телефонные переговоры, остается важнейшим каналом информационного взаимодействия. Зачастую развитие и введение в эксплуатацию новых систем связи направлено на совершенствование именно этого метода общения. Одновременно усиливается потребность в обеспечении конфиденциальности речевого обмена и защите информации, имеющей речевую природу.

В настоящий момент разработан достаточно широкий арсенал различных средств защиты (формальных и неформальных), которые могут обеспечить требуемый уровень защищенности разного рода информации, в том числе и речевой. Развитие неформальных средств защиты (законодательных, организационных, морально-этических и т.п.) проводится в рамках общего законодательного процесса и посредством совершенствования соответствующих инструкций.

В России сложилась достаточно разветвленная правовая система, которая регламентирует многие аспекты организации и обеспечения информационной безопасности [1]. Важное место в этой системе занимают требования по лицензированию и сертификации, но возможность применения этих требований к защите собственных информационных ресурсов в собственных же интересах не очевидна [2]. Есть определенные правовые коллизии и в широком применении ряда криптографических средств, строго говоря, не прошедших сертификацию в России, но использующихся в глобальных системах связи.

Причины такого положения, видимо, кроются в необходимости применения различных критериев, в том числе и правовых, в вопросах сертификации коммерческих систем связи (требования по защите информации в коммерческих целях) и систем связи специального назначения (требования по защите гостайны).

На развитие и совершенствование арсенала технических средств защиты речевой информации оказывают влияние многочисленные объективные и субъективные факторы, основные из которых сформулированы ниже.

F1. Речевой и слуховой аппарат человека является прекрасно сопряженной и исключительно помехоустойчивой системой. Поэтому подавление смыслового восприятия речи происходит при отношении шум/сигнал в несколько сотен процентов, а подавление признаков речи (т.е. невозможность фиксации факта разговора) достигается при отношении шум/сигнал ≈ 10 и выше [2, 3].

F2. Аппаратура и системы связи, связанные с обработкой и передачей речевой информации, постоянно совершенствуются и развиваются. Для мобильных телефонов и наладочных компьютеров речевой интерфейс является самым удобным способом обмена информацией. Соответствующие изменения затрагивают как возможные каналы утечки речевой информации, так и методы получения несанкционированного доступа (НСД) к этой информации. Эти процессы требуют адекватной реакции при разработке стратегии защиты и совершенствовании методов защиты речевых сигналов.

F3. Широкое распространение получают принципиально новые автоматизированные и компьютеризованные системы обработки, в которых происходит обработка, накопление и хранение огромных массивов информации, в том числе имеющих речевую природу (записи переговоров, речевая почта, данные акустического контроля и т.п.). В связи с этим требуется разработка технологий и методов защиты речевой информации, передача которой по каналам связи не предполагается.

F4. Постоянно развиваются методы и совершенствуется аппаратура для получения несанкционированного доступа к речевой информации, в частности к телефонным переговорам. В силу своей специфики и протяженности системы связи, предоставляющие услуги телефонных переговоров и речевого общения, являются наиболее уязвимыми для НСД и утечки конфиденциальной информации.

F5. Интеграция России в мировую экономическую систему и динамичное развитие бизнеса, который по своей природе стремится формировать и заполнять имеющиеся пробелы в сфере услуг, приводят к появлению хорошо оснащенных фирм, имеющих значительные технические возможности по НСД к конфиденциальной информации. Это, в свою очередь, меняет модель противника – один из важнейших параметров, которые необходимо рассматривать при разработке мер защиты.

Традиционно рассматривают две основных задачи, которые необходимо решить для предотвращения утечки конфиденциальной речевой информации.

Z1. Задача обеспечения безопасности переговоров в помещении или в пределах контролируемой территории.

Z2. Задача обеспечения защиты речевой информации в канале связи.

Основные факторы, перечисленные выше, позволяют говорить по крайней мере еще о двух направлениях, по которым необходима организация специальных мероприятий и мер защиты.

Z3. Обеспечение постоянного контроля эффективности защиты речевой информации с целью предотвращения появления новых каналов утечки при кажущемся достаточным уровне защиты.

Z4. Накопление и хранение в защищенном виде массивов различной информации, имеющей речевую природу. Сюда же, видимо, следует отнести и информацию мультимедийного характера.

Для решения задачи Z4 можно применять стандартные методы, позволяющие накапливать и хранить в защищенном виде информацию конфиденциального характера. Но специфика объекта защиты и требования к работе с записями речевых переговоров вынуждают рекомендовать использовать для этих целей отдельные защищенные помещения, вычислительные средства и специальные информационно-справочные и информационно-поисковые системы.

Каналы телефонной связи являются наиболее уязвимыми с точки зрения организации НСД к конфиденциальной информации. Контролировать телефонные переговоры можно на всем протяжении телефонной линии, а при использовании мобильной связи еще и во всей зоне распространения радиосигнала [4 – 6].

В настоящее время можно говорить о следующих видах телефонной связи:

- стандартная телефонная связь, которая осуществляется по коммутируемым каналам;
- мобильная связь, основным примером которой можно считать связь по стандарту GSM;
- цифровая телефония (IP-телефония), которая осуществляется по сетям с коммутацией пакетов.

Каждый вид телефонной связи имеет свои особенности, которые необходимо учитывать при построении концепции защиты информации.

Штатная концепция защиты речевых переговоров при стандартной телефонной связи состоит в предположении отсутствия у злоумышленника доступа к телефонным каналам. Каких-либо средств защиты данная система телефонной связи не предусматривает. При отсутствии уверенности в такой «системе» защиты решение задачи обеспечения безопасности переговоров полностью ложится на абонентов.

В основе концепции защиты информации в системе связи стандарта GSM лежат криптографические протоколы аутентификации, алгоритмы шифрования трафика в радиоканале и система временных идентификаторов абонентов [7]. Все эти средства защиты обеспечиваются самой системой связи.

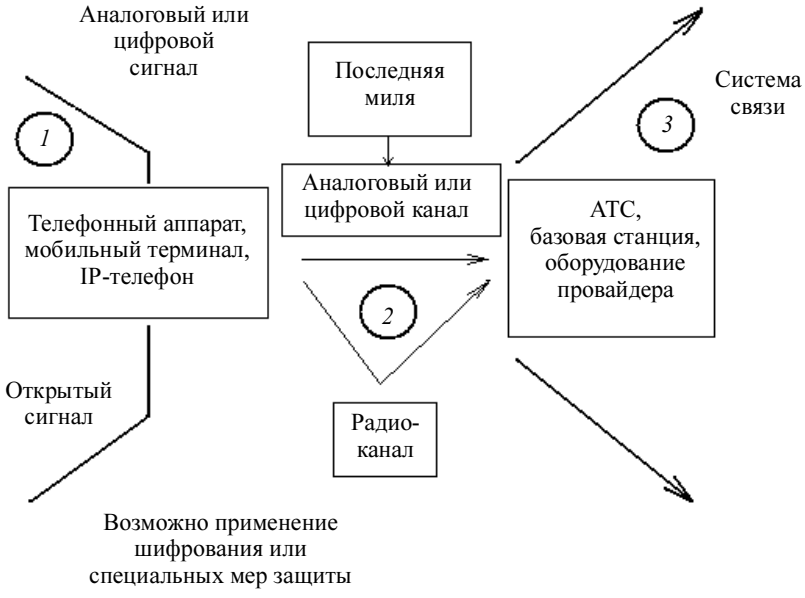

Рис.1. Общая модель телефонной связи

Цифровая телефония допускает применение практически всего спектра средств криптозащиты (защищенные протоколы, шифрование трафика и т.п.), причем это может обеспечиваться как штатными средствами защиты системы связи (провайдера), так и оборудованием абонентов.

Для пользователя все три вида телефонного обслуживания представляются как единая телефонная сеть, и он зачастую не знает, как точно осуществляется то или иное телефонное соединение. Поэтому логично для рассмотрения вопросов обеспечения безопасности схематично представить укрупненную модель телефонной связи (рис. 1).

Цифрами обозначены «точки» (места), в которых условия доступа к речевым сигналам с целью НСД имеют принципиальные отличия.

Т о ч к а *1*. Помещение, пространство на улице и т.п., в котором абонент непосредственно осуществляет телефонное общение.

Данная точка характеризуется следующими основными особенностями:

• наличием открытого речевого сигнала (не зашифрованного) в аналоговой форме;

• при телефонном разговоре имеется (слышен) сигнал только одного абонента;

• имеются определенные ограничения по возможностям применения средств защиты (средства как минимум не должны мешать ведению переговоров), невозможно использовать криптографические методы защиты.

Т о ч к а *2*. Канал связи – аналоговый, цифровой или радиоканал – между терминалом абонента и оборудованием системы связи. Для стандартной телефонной связи это АТС. Для мобильной связи – базовая станция. Для IP-телефонии – оборудование провайдера.

Точка характеризуется:

• в определенной степени постоянным и достаточно стабильным каналом связи, который невозможно обеспечить физической защитой на всем протяжении;

• сигнал может иметь аналоговую или цифровую форму, быть открытым или зашифрованным;

• в коммутируемом канале связи присутствуют одновременно сигналы обоих абонентов [8];

• можно использовать практически любые средства защиты, включая криптографические протоколы аутентификации и многоуровневое шифрование [2, 6, 9, 10].

Т о ч к а *3*. Оборудование и каналы той или иной системы связи.

Главная цель выделения точки *3* состоит в необходимости подчеркнуть факт, что условия осуществления НСД к телефонным переговорам «внутри» системы связи имеют место быть, и они могут принципиально отличаться от условий осуществления НСД на «последней» миле (в точке *2*). Причем эти условия могут быть как значительно проще, так и значительно сложнее. Но в любом случае для осуществления НСД в точке *3* необходимо иметь доступ к штатному оборудованию системы связи (оборудованию провайдера).

В точке *1* необходимо обеспечить решение задач Z1 и Z3.

Задача защиты переговоров, происходящих в помещении или на контролируемой территории, всегда может быть решена ценой определенных затрат и с созданием больших или меньших неудобств для переговаривающихся персон [2, 10]. Это обеспечивается:

- проверкой помещения и определенным контролем прилегающей территории, использованием технических средств (розеток, телефонных аппаратов, оргтехники и т.п.), исключающих утечку информации по побочным каналам;

- организацией соответствующего режима доступа в проверенное и контролируемое помещение;

- применением средств физической защиты информации, включающих в себя постановщики заградительных помех, нейтрализаторы, фильтры и средства физического поиска каналов утечки информации. Причем желательно обеспечить создание некоррелированных помех, исключающих возможность их компенсации при многоканальном съеме информации [11];

- постоянным мониторингом и оценкой качества защиты речевой информации на объекте. Существует много объективных и субъективных причин, которые могут явиться источником сбоев и нарушений в функционировании систем защиты в рабочих помещениях.

Очевидно, приведенная выше система мер в основном направлена на обеспечение безопасности связи со стационарных телефонов (в том числе и IP) и на предотвращение утечки по побочным каналам, одной из причин которых может являться телефон мобильной связи. Безопасность телефонных переговоров вне контролируемого помещения и в мобильном варианте эта система мер не обеспечивает.

Для предотвращения НСД к речевой информации в точке *2* можно использовать практически любые технические средства. В частности, для защиты обычных телефонных каналов сегодняшний рынок представляет пять разновидностей специальной техники [10, 12]:

- анализаторы телефонных линий;

- средства пассивной защиты;

- постановщики активной заградительной помехи;

- односторонние маскираторы речи [13];

- криптографические системы защиты [6, 9, 14].

Предназначение технических средств, относящихся к первым трем группам, достаточно очевидно.

Принято выделять три типа устройств [15], обеспечивающих криптографическую защиту речевой информации: маскираторы, скремблеры и устройства с передачей шифрованной речи в цифровом виде. Маскираторы и скремблеры относятся к аппаратуре временной стойкости [2, 9], так как используют передачу преобразованного сигнала по каналу связи в аналоговом виде. Вообще, провести строгое обоснование степени защищенности скремблеров крайне сложно.

Для гарантированной защиты телефонных переговоров желательно использовать аппаратуру, построенную на принципах цифровой передачи речи и обеспечивающую криптографическую защиту на всех этапах передачи.

Таким образом, оба абонента телефонной связи должны быть оснащены соответствующей шифртехникой, что является определенным неудобством. Вторым важным недостатком является тот факт, что в настоящее время ни один из скремблеров [12] не имеет надежной системы предотвращения перехвата речевой информации из помещения по телефонной линии, находящейся в отбое. Следовательно, такая аппаратура предоставляет принципиальную возможность проводить НСД в точке *1* (см. рис. 1) по техническим каналам утечки: акустическому, электромагнитному, сетевому и др.

В какой-то степени решить вопросы защиты речевого обмена в точке *2* позволяют односторонние маскираторы [13], но говорить о полной, надежной и доказательной защите информации в этом случае нет оснований.

Для защиты в точке *2* сигналов IP-телефонии из приведенного выше списка специальной техники можно использовать анализаторы телефонных линий (для контроля над возможными несанкционированными подключениями к линии) и цифровые системы криптографической защиты. Применение технических средств, вносящих помехи в канал связи, приведет к разрушению цифрового канала и невозможности использования IP-телефонии.

Как видно из рис. 1, концепция защиты информации сотовых систем, по сути, ограничивается только точкой *2* (т.е. радиоканалом). О мерах по дальнейшей защите должны позаботиться сами абоненты. Решить эти вопросы можно путем применения специальных криптографических средства абонентского шифрования, которые позволяют защищать речевой сигнал на всем пути следования от одного мобильного терминала до другого.

Применение подобных криптографических средств позволяет защищать речевую информацию в телефонных проводах, системах связи IP-телефонии и сотовых сетях. По сути, это единственная возможность построения надежной (и доказательной) системы защиты речевых переговоров в точках *2* и *3*.

Таким образом, надежное перекрытие возможных каналов утечки в охраняемых помещениях и применение сертифицированных криптографических средств, позволяющих шифровать информацию на всем протяжении линий связи между абонентами, позволяет построить надежную систему защиту для конфиденциального обмена речевой информацией. Правомерность таких рекомендаций подтверждают и некоторые публикации [16], в которых рассматриваются зарубежные технологии и терминология доступа к конфиденциальной информации. Доступ к данным в точке *1* характеризуется как доступ к открытой информации – «информации в покое» (information at rest). В противоположном состоянии – «информация в движении» (info in motion), открытый текст может быть зашифрован сильным криптоалгоритмом, и быстро подступиться к нему уже невозможно.

ЛИТЕРАТУРА

1. *Развитие* правового обеспечения информационной безопасности / Под ред. А.А. Стрельцова. М.: Престиж, 2006.
2. *Кравченко В.Б.* Защита речевой информации в каналах связи // Специальная техника. 1999. № 4. С. 2 – 9; 1999. № 5. С. 2 – 11.
3. *Цвикер Э.*, *Фельдкеллер Р.* Ухо как приемник информации / Пер. под общ. ред. Б.Г. Белкина. М.: Связь, 1971.
4. *Закрытие* телефонных переговоров. ВЕБ форум по безопасности. http://www.sec.ru/
5. *Материалы* сайта http://www.Phreaking.RU/
6. *Sutton R.J.* Secure Communications: Applications and Management. John Wiley & Sons, 2002.
7. *Ратынский М.* Телефон в кармане. Путеводитель по сотовой связи. М.: Радио и связь, 2000.
8. *Лагутенко О.И.* Модемы: Справочник пользователя. СПб.: Лань, 1997.
9. *Алферов А.П.*, *Зубов А.Ю.*, *Кузьмин А.С.*, *Черемушкин А.В.* Основы криптографии. М.: Гелиос АРВ, 2001.
10. *Петраков А.В*. Основы практической защиты информации. М.: Радио и связь, 1999.
11. *Бортников А.Н.*, *Губин С.В.*, *Комаров И.В.*, *Майоров В.И.* Совершенствование технологий информационной безопасности речи // Конфидент. 2001. № 4.
12. *Сталенков С.* Способы и защита телефонных линий. http://daily.sec.ru/
13. *Абалмазов Э.И.* Новая технология защиты телефонных переговоров // Специальная техника. 1998. № 1. С. 3 – 9.
14. *Beker H.J.*, *Piper F.C.* Secure Speech Communications. London: Academic Press, 1986.
15. *Смирнов В.* Защита телефонных переговоров // Банковские технологии. 1996. № 8. С. 5 – 11.
16. *Берд К.* Искусство быть // Компьютерра. 2005. №11. http://www.computerra.ru/offline/2005/583/38052/