Защита информации в телекоммуникациях. Новые тенденции.

Сборник материалов Всероссийской конференции
Информационная безопасность России в условиях глобального информационного сообщества, Москва, 2001

В настоящее время одной из основных предпосылок прогрессивного развития общества является владение и правильное распоряжение информационными ресурсами, которые представляют собой объекты отношений физических, юридических лиц и государства. В пределах своей компетенции собственнику предоставляется право самостоятельно устанавливать режим защиты информационных ресурсов и доступа к ним.

К сожалению, в силу недостаточной информированности большинство российских граждан не видит для себя проблемы информационной безопасности. И деятельность в этой области ограничена относительно узким кругом специалистов и фирм, предлагающих в этом секторе рынка свои услуги и технические средства. Между тем, такая проблема существует, и с развитием информационных технологий становится все более и более актуальной. Ведь любая информация, не носящая массового характера и предназначенная для ограниченного круга лиц, попадая в руки злоумышленника, может быть использована им во вред. При этом содержание информации, на первый взгляд, может носить безобидный характер. Злоумышленник может использовать буквально все: от сведений чисто бытового характера до информации, содержащей служебную и коммерческую тайну. В достаточной степени трудно объяснить человеку, не имеющему практически никаких материальных подтверждений производимых им финансовых затрат, что в будущем эти затраты многократно окупятся. Большинство продолжают жить, надеясь на 'авось', и обращаются к специалистам только после ощутимых финансовых потерь. В этот момент перед ними встает ряд сложных, требующих разрешения проблем. Прежде всего, это выбор предприятия или фирмы, способной оптимально с уровнем необходимой достаточности и кондифициальности решать поставленные задачи.Эти задачи могут быть решены как техническими,так и организационными мерами, а в большинстве случаев сочетанием этих мер. Вторая проблема состоит в выборе необходимых технических средств.

В настоящее время на рынке предлагается огромное количество устройств, способных в той или иной степени решать проблемы информационной безопасности. Степень их эффективности, как и ценовые характеристики, колеблются в очень широком диапазоне. Поэтому, прежде чем преступить к формированию парка необходимых технических средств, необходимо произвести условное моделирование потенциального противника, т.е. того, от кого должна быть установлена защита, сделать примерную оценку его технических и интеллектуальных возможностей в этой области. Такая оценка поможет оптимально сконфигурировать создаваемую систему информационной безопасности и избежать ненужных материальных затрат.

Следует отметить, что решение проблемы информационной безопасности является комплексной задачей, и бессистемное приобретение отдельных технических средств, как правило, приводит к неэффективным затратам финансовых средств с минимальными результатами. Поэтому не следует делать никаких приобретений без серьезной консультации со специалистами. Более того, практика некомплексного подхода к обеспечению информационной безопасности приводит к дискредитации самой возможности решения проблемы защиты информации.

Интенсивное развитие средств и систем передачи речевой информации делает все более актуальной проблему обеспечения ее безопасности. Для обеспечения безопасности связи используются специальные технические средства, методы и организационные мероприятия для предотвращения потери, утечки, хищения, искажения, подделки информации.

В свете решения этой задачи одним из наиболее важных направлений является шифрование речевой информации. Два основных метода, используемых для защиты речевых сигналов широко известны: это аналоговое скремблирование и преобразование речи в низкоскоростной цифровой поток данных с последующим шифрованием. У каждого из этих методов были свои преимущества и недостатки. Так аналоговые скремблеры отличались более высоким качеством восстановленной на приеме речи, невосприимчивостью к фазовым характеристикам канала связи, однако, имели значительно более низкую криптостойкость и создавали временные задержки речевого сигнала, затрудняющие диалог абонентов. В течение многих лет делались попытки организовать речевую передачу информации таким образом, чтобы закрыть ее от несанкционированных лиц. В этом плане наиболее широко используются методы, с помощью которых меняются местами частотные диапазоны и временные интервалы речевого сигнала. Наличие в канале связи речи позволяет противнику атаковать эти системы на уровне анализа звуковых сигналов. При этом может быть использован минимальный набор общедоступных технических средств. Результатом подобной атаки в настоящее время является полное восстановление зашифрованного сообщения в реальном времени без каких-либо задержек. Более того, стало бессмысленным наличие в подобных системах огромного количества ключевых установок, так как противник не занимается и не будет заниматься их прямым перебором. Если 2-3 года тому назад расшифровка таких сообщений являлась лишь делом времени, то сегодня этого времени нет. Безопасность, достигаемая использованием методов 'перестановки' настолько ограничена, что их использование сможет защитить информацию только от прямого случайного прослушивания. Если вспомнить о необходимости защиты факсимильной информации, то ее подобными методами вообще защитить нельзя, так как деление линейного сигнала факсимильного модема на последовательность временных сегментов приводит к необратимым потерям фазовых характеристик сигнала. В данном случае единственно приемлемым является метод частотной инверсии спектра несущей частоты факсимильного модема. При этом частота инверсии должна быть фиксированной на весь сеанс связи. При атаке на такой сигнал значение частоты, соответствующей средней точке инверсии определяется без труда. В результате уровень защиты оказывается крайне низким. Еще одним потерянным преимуществом аналоговых систем является качество восстановленной на приеме речи.

Появление современных, высоко производительных сигнальных процессоров обусловило возможность реализации высокосложных алгоритмов сжатия речевого сигнала. При этом потери качества речи при ее синтезе на приеме полностью отсутствуют. Иными словами, при разговоре абонент не только не чувствует ухудшения качества речи, но и в ряде случаев отдает предпочтение закрытому режиму по сравнению с открытым.

Достигается это применением методов цифровой передачи речевого сигнала с высокой информационной эффективностью. Использование широко известной технологии CELP позволило создать авторизированный, низкоскоростной(4800бит\сек) алгоритм преобразования речевого сигнала в цифровой поток данных с применением

методов векторного кодирования и комбинаторным возбуждением.

Развитие телекоммуникационных систем и совершенствование связных протоколов для модемов передачи данных позволило реализовать устройство, устойчиво работающее на любых каналах коммутируемой сети связи общего пользования.

Совершенно очевидно, что в современных условиях основным методом защиты информации в сетях связи является ее преобразование в цифровой поток с последующим шифрованием и передачей по каналу модемными методами.

При создании устройтсв, претендующих на определенный уровень гарантированности защиты информации, появляется ряд алгоритмических, математических, схемо-технических, юридических и психологических проблем. От того, на сколько грамотно и профессионально они будут решены, зависит безопасность информации в целом, широта распространения этой техники на рынке средств защиты информации, возможность сотрудничества и здоровой конкуренции с другими производителями.

Следует заметить, что правильный выбор и корректная реализация алгоритма шифрования является лишь частью проблем, которые необходимо решить при создании аппаратуры, претендующей на определенные гарантии в деле защиты информации. Дело в том, что сам по себе аппарат в процессе работы может создавать возможность утечки информации по различным техническим каналам: электромагнитному, акустоэлектрическому, сетевому и т.п. Поэтому создание аппаратуры гарантированной стойкости, предназначенной для защиты сведений, составляющих государственную тайну, является прерогативой научно-технических подразделений ФАПСИ, ФСБ, Министерства обороны и др.

Только они в полной мере отвечают требованиями, предъявляемыми к этой аппаратуре, а также методиками и техническими средствами для их проверки.

Под гарантированной стойкостью подразумевается, что информация, переданная с помощью этой аппаратуры, не может быть получена противником при использовании им любых технических средств (с учетом прогресса) в течение срока хранения государственной тайны 30-50 лет.

Такая аппаратура имеет очень высокие ценовые характеристики, и ее эксплуатация требует постоянного проведения целого комплекса организационных мероприятий, обеспечивающих безопасность информации.

К тому же любая организация, желающая использовать эту аппаратуру, обязана получить лицензию ФАПСИ на право эксплуатации криптографической техники.

В связи с этим возникает вопрос: а так ли уж необходим коммерческим организациям такой высочайший уровень защиты информации. Может быть, достаточно остановиться на 5-10 годах гарантии защищенности информации в канале связи. Возможно ли дать подобные гарантии без использования традиционных методов шифрования и криптографии в их классическом понимании?

Если определить шифр как недопустимое для восприятия отображение открытой информации, то это понятие очень широко. Под него попадает огромное количество алгоритмических преобразований, таких как кодирование, архивирование и т.д. Для уточнения следует определить основной признак шифрования - это наличие такого компонента как 'ключ'. Сам процесс формирования, копирования, рассылки, установки и учета ключевой информации помимо организационных создает и чисто технические проблемы в виде появления новых возможных каналов утечки информации.

Организационные требования, предъявленные к защищаемой системе связи, в подавляющем большинстве коммерческих организаций просто не выполняется.

Для проведения анализа линейного сигнала противнику требуется создать банк данных, основанный на записях перехваченных закрытых сеансов связи. Таких сеансов должно быть не менее нескольких десятков тысяч. Естественно, на это требуется значительное время. Следовательно, общая стойкость систем впрямую связана с количеством аппаратуры и сеансов связи. Однако это вовсе не означает, что стойкость системы будет низкой; при использовании комплекса мер и алгоритмов кодирования она будет близка к гарантированной. К этим мерам следует отнести:

- применение многоэтапного кодирования со случайно формируемым алгоритмом;
- работу в полностью изолированной программной среде;
- постоянное тестирование и контроль за работой системы;
- аутентификацию аппаратов в системе и проверку целостности средств защиты;
- защиту программного обеспечения от преднамеренного и непреднамеренного вмешательства.

Одной из основных задач, стоящих перед разработчиком, является формирование линейного сигнала. При этом вид и состав этого сигнала должен быть таким, что для получения из него исходной информации противнику пришлось бы проделать количество математических операций, соизмеримое с атакой на криптосистему в 'лоб', т.е. заниматься прямым перебором ключей. И если такое количество превышает величину 10^{17}, то такой линейный сигнал можно считать надежно защищенным. Именно этот путь и был избран при создании микропроцессорного телефонного терминала SP19/ДТ.

Микропроцессорный телефонный терминал SP-19/DT предназначен для организации цифровых каналов передачи речевой и факсимильной информации, а также для ее автоматической защиты в режиме 'абонент-абонент'. При этом в качестве транспортной используется коммутируемая телефонная сеть общего пользования с двухпроводным окончанием.

Состав программно-реализованных технических средств терминала:

Речепреобразующее устройство предназначено для представления речевого сигнала в виде низкоскоростного цифрового потока на передаче и синтеза речи на приёме. При этом качество восстановленной речи практически не отличается от обычного телефонного разговора. Процедура реализована на основе модернизированного алгоритма CELP. Алгоритм CELP (Code Excited Linear Prediction), построен на модели кодирования с использованием процедуры анализа-через-синтез, линейного предсказания и векторного квантования. Для моделирования кратковременного спектра речевого сигнала (формантной структуры) используется фильтр линейного предсказания 10-го порядка. Для формирования сигнала возбуждения используются адаптивная и стохастическая кодовые книги. Вычислительная сложность алгоритма определяется процедурами поиска оптимальных векторов возбуждения по двум кодовым книгам. Таким образом, CELP анализ состоит из трёх основных процедур:

- кратковременное линейное предсказание,
- долговременный поиск по адаптивной кодовой книге,
- поиск по стохастической кодовой книге.

CELP синтез состоит из этих же процедур, выполненных в обратном порядке. Кодер оперирует с кадрами речевого сигнала длиной 30 мс (240 отсчетов), дискретизованными с частотой 8КГц. В свою очередь, каждый из этих кадров делится на четыре подкадра по 60 отсчетов. Для каждого кадра производится анализ речевого сигнала, и выделяются передаваемые параметры CELP-модели: 10 линейных спектральных пар (несут информацию о коэффициентах фильтра линейного предсказания), индексы и коэффициенты усиления в адаптивной и фиксированной кодовых книгах. Далее эти

параметры кодируются в битовый поток и передаются в канал.

В декодере эта битовая посылка используется для восстановления параметров сигнала возбуждения и коэффициентов синтезирующего фильтра. Далее восстанавливается речь, путем пропускания сигнала возбуждения через синтезирующий фильтр. Затем для улучшения качества восприятия синтетического сигнала выходной сигнал с фильтра-синтезатора пропускается через постфильтр.

Разборчивость восстановленной речи 99% при полной узнаваемости разговаривающих абонентов. Динамический диапазон не менее 60 дБ. Суммарные задержки речевого сигнала 100 мс. Скорость работы 4800 бит/сек.

Синхронный модем с оригинальным протоколом для передачи и приёма речевой информации по каналу связи. Время восстановления синхронизации в зависимости от качества канала связи до 5 сек. Скорость работы до 4800 бит/сек.

Станционный факсимильный модем предназначен для преобразования линейного сигнала факсимильного аппарата в цифровой поток с целью его последующей защиты на передаче и обратных преобразований на приёме. Протоколы V21, V27, V27ter, V29 МККТТ.

Линейный факсимильный модем предназначен для передачи и приёма защищенной факсимильной информации по каналу связи. Рекомендации Т30 МККТТ, протоколы V21, V27, V27ter, V29. Время установления соединения определяется качеством канала связи и возможностями факсимильных аппаратов.

Узел кодирования предназначен для преобразования цифровых информационных потоков в вид недоступный для потенциального противника. Информация реорганизуется по случайно выбранному алгоритму, в процессе сеанса программирования, каждой отдельной группы аппаратов.

Система управления индикации и тестирования предназначена для:

- программирования терминалов различной конфигурации;
- защиты программного обеспечения терминала;
- программирования пользовательских функций;
- управления режимами работы при помощи факсимильных протоколов и сигналов DTMF;
- самотестирования всех технических средств терминала при отсутствии соединения и индикации результатов;
- индикации рабочего режима.

Безопасность информации в канале связи обеспечивается применением многоэтапного кодирования в процессе ее обработки, при этом все алгоритмы оригинальны и не имеют аналогов.

- параметрическое кодирование речевой информации для преобразования аналогового речевого сигнала в цифровой поток данных.
- сжимающее кодирование цифрового потока данных для минимизации количества передаваемой информации на принципах линейного предсказания.
- линейное кодирование для реорганизации цифрового потока данных по случайно выбранному алгоритму.
- внесение псевдослучайностей в передаваемый сигнал для улучшения настройки и адаптации в рабочем режиме.
- помехоустойчивое кодирование с применением сигнально-кодовой конструкции.

Безопасность программного обеспечения необходима для создания условий неприкосновенности данных в процессе их хранения и использования. В SP-19/DT используются ряд мер, обеспечивающих очень высокую степень защищенности программного обеспечения. Информация не может быть считана даже разработчиком, она может быть только обновлена.

Безопасность сети связи обеспечивается:

1. Аутентификацей абонента в системе на основе технологии цифровой подписи электронных данных;
2. Применением для каждой группы аппаратов алгоритма линейного кодирования для реорганизации электронных цифровых потоков.

Уникальность алгоритма заключается в том, что он создается только один раз в едином для каждой группы аппаратов сеансе программирования и больше никогда не может быть повторен. Единый сеанс программирования формирует одну группу аппаратов с общим алгоритмом кодирования. В процессе программирования случайно выбирается один из огромного количества вариантов реорганизации информационного цифрового потока. При этом этот вариант неизвестен никому (пользователю, производителю, противнику). Он не может быть считан из памяти аппарата и подлежит только обновлению. Пользователь формирует идентификатор, предназначенный для определения "своего" аппарата в группе в процессе синхронизации. Аппарат, запрограммированный в другом сеансе, не может работать в данной группе даже при наличии у него аналогичного идентификатора. Следовательно, различные группы аппаратов не могут работать между собой.

Следует отметить, что оригинальность схемотехнических и алгоритмических решений, использованных при создании микропроцессорного телефонного терминала, а также общая идеология построения системы позволяют реализовать новые перспективные разработки.

В настоящее время проводятся линейные испытания аппаратуры, предназначенной для защиты информации в сетях сотовой связи. При этом обеспечивается стык с существующей моделью аппарата. В стадии разработки находится модель, позволяющая защищать информацию в сетях IP, X.225, Frame Relay, обеспечивая их соединение с существующей сетью связи общего использования.

Все это позволяет надеяться, что микропроцессорный телефонный терминал займет одно из лидирующих мест на рынке техники защиты информации в телекоммутационных системах.