Защита каналов связи

В этой главе

- *Криптографические методы и средства защиты информации*
- *Защита данных при передаче по каналам связи ИС*
- *Защищенный обмен сообщениями*
- *Защита электронной почты*
- *Защита телефонных линий от прослушивания*
- *Способы и средства защиты телефонных переговоров*

<<< Этапы	Направления >>>	010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				ПЭМИН				Управление системой защиты			
	Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных мер и средств	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

Защита каналов связи занимает особое место в общей структуре комплексной системы защиты информации (рис. 14.1).

Информация должна оставаться конфиденциальной как в процессе ее перемещения в пределах внутренней сети, так и при передаче в другие ИС. Никогда нельзя исключить возможность "подслушивания" данных, передаваемых по проводным каналам связи. А перехват "открытой информации", передаваемой по линиям сотовой и радиорелейной связи, является для технически подготовленного злоумышленника еще более легкой задачей.

Криптографические методы и средства защиты информации (034)

Необходимость надежной защиты информации потребовала криптографических средств защиты информации.

Криптографическими средствами защиты называются специальные методы и средства преобразования информации, в результате которых маскируется ее содержание.

Основными видами криптографического закрытия являются шифрование и кодирование защищаемых данных. При этом ***шифрование*** есть такой вид закрытия, при котором самостоятельному преобразованию подвергается каждый символ закрываемых данных; ***при кодировании*** защищаемые данные делятся на блоки, имеющие смысловое значение, и каждый такой блок заменяется цифровым, буквенным или комбинированным кодом.

Для криптографического закрытия информации в системах обработки данных наибольшее распространение получило шифрование. Используется несколько систем шифрования: замена (подстановка), перестановка, гаммирование, аналитическое преобразование шифруемых данных. Широкое распространение получили комбинированные шифры, когда исходный текст последовательно преобразуется с использованием двух или даже трех различных шифров. Например, комбинированное применение замены и гаммирования или перестановки и гаммирования и т.п.

Надо знать

Основной характеристикой меры защищенности информации криптографическим закрытием является стойкость шифра, когда *под стойкостью понимается тот минимальный объем зашифрованного текста, статистическим анализом которого можно вскрыть исходный текст*. Таким образом, по значению стойкости системы шифра можно определить допустимый объем шифрования информации при одних и тех же ключевых установках. Простые системы шифрования (простая замена, простая перестановка) обладают незначительной стойкостью, вследствие чего они могут использоваться лишь для шифрования коротких сообщений. Усложненные виды замены и перестановки имеют значительно большую стойкость, стойкость же гаммирования определяется лишь размером гаммы (случайной последовательности, используемой для шифрования). Если для шифрования используется бесконечная случайная последовательность, то такой шифр теоретически — абсолютно стоек, т.е. нераскрываем.

Однако применение такого шифра сопряжено с большими трудностями, поэтому в реальных системах этот вид шифрования не встречается. Большое распространение получили комбинированные шифры, их стойкость теоретически равна произведению стойкости используемых простых шифров.

Важная характеристика системы шифрования — ее производительность. ***Производительность шифрования*** зависит как от используемой системы шифра, так и от способа реализации шифрования аппаратного или программного. С точки зрения трудоемкости шифрования наименьших затрат требуют шифры замены, а наибольших — шифры, основанные на аналитическом преобразовании данных. С точки зрения способа реализации, производительность аппаратного шифрования в несколько раз превышает производительность программного шифрования, поэтому первому уделяется особое внимание. В то же время, программное шифрование обладает большими возможностями по использованию различных методов и при современных сред-

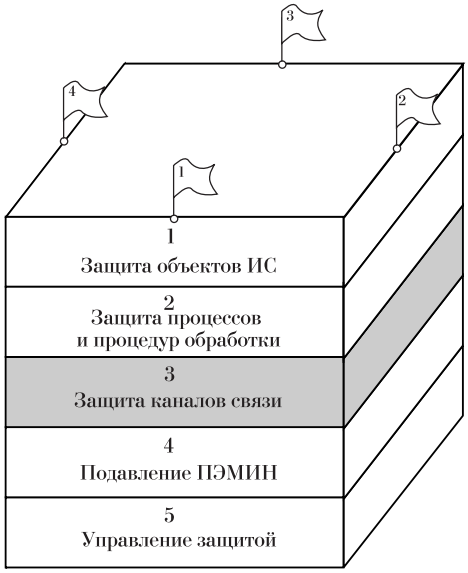


РИС. 14.1. *Место вопросов защиты каналов связи в общей структуре СЗИ.*

ствах (высокая тактовая частота) применение программных методов также достаточно эффективно и очень часто применяется в средствах вычислительной техники наряду с другими программными средствами защиты информации.

Основные сведения о криптографии (031)

Под криптологией (от греческого kruptos — тайный и logos сообщение) понимается наука о безопасности (секретности) связи.

Криптология делится на две части: криптографию (шифрование) и криптоанализ. ***Криптограф*** пытается найти методы обеспечения секретности и или аутентичности (подлинности) сообщений. ***Криптоаналитик*** пытается выполнить обратную задачу: раскрыть шифртекст или подделать его так, чтобы он был принят как подлинный.

Одним из основных допущений криптографии является то, что криптоаналитик противника имеет полный шифртекст и ему известен алгоритм шифрования, за исключением секретного ключа. При этих допущениях криптограф разрабатывает систему, стойкую при анализе только на основе шифротекста. На практике допускается некоторое усложнение задачи криптографа. Криптоаналитик противника может иметь фрагменты открытого текста и соответствующего ему шифротекста. В этом случае криптограф разрабатывает систему стойкую при анализе на основе открытого текста. Криптограф может даже допустить, что криптоаналитик противника способен ввести свой открытый текст и получить правильный шифртекст с помощью секретного ключа (анализ на основе выбранного открытого текста), и наконец, — объединить две последние возможности (анализ на основе выбранного текста).

Многие из стратегий нарушителя могут быть блокированы с помощью криптографических средств защиты информации, но следует отметить, что большинство стратегий нарушителя связано с проблемами аутентичности пользователя и сообщений. Что это означает?

Подсистема криптографической защиты (032)

Подсистема объединяет средства криптографической защиты информации и предназначена для обеспечения целостности, конфиденциальности, аутентичности критичной информации, а также обеспечения юридической значимости электронных документов в ИС. По ряду функций подсистема кооперируется с подсистемой защиты от НСД. Поддержку подсистемы криптографической защиты в части управления ключами осуществляет подсистема управления СЗИ.

Структурно подсистема состоит из:

- программных средств симметричного шифрования данных;
- программно-аппаратных средств цифровой подписи электронных документов (ПАС ЦП).

Функции подсистемы предусматривают:

- обеспечение целостности передаваемой по каналам связи и хранимой информации;
- имитозащиту сообщений, передаваемых по каналам связи;
- скрытие смыслового содержания конфиденциальных сообщений, передаваемых по каналам связи и хранимых на носителях;
- обеспечение юридической значимости электронных документов;
- обеспечение аутентификации источника данных.

Функции подсистемы направлены на ликвидацию наиболее распространенных угроз сообщениям в автоматизированных системах:

- ***угрозы, направленные на несанкционированное ознакомление с информацией:***
  - несанкционированное чтение информации на машинных носителях и в ЗУ ЭВМ;
  - незаконное подключение к аппаратуре и линиям связи;
  - снятие информации на шинах питания;
  - перехват ЭМИ с линий связи;
- ***угрозы, направленные на несанкционированную модификацию (нарушение целостности) информации:***
  - изменение служебной или содержательной части сообщения;
  - подмена сообщения;
  - изъятие (уничтожение) сообщения.
- ***угрозы, направленные на искажение аутентичности отправителя сообщения:***
  - незаконное присвоение идентификаторов другого пользователя, формирование и отправка электронного документа от его имени (маскарад), либо утверждение, что информация получена от некоего пользователя, хотя она сформирована самим нарушителем;
  - повторная передача документа, сформированного другим пользователем;
  - искажение критичных с точки зрения аутентичности полей документа (даты формирования, порядкового номера, адресных данных, идентификаторов отправителя и получателя и др.).
- ***угрозы, связанные с непризнанием участия:***

- отказ от факта формирования электронного документа;
- отказ от факта получения электронного документа или ложные сведения о времени его получения;
- утверждение, что получателю в определенный момент была послана информация, которая в действительности не посылалась (или посылалась в другое время).

Аутентичность сообщений (034)

Конечной целью шифрования является обеспечение защиты информации от несанкционированного ознакомления, аутентификации обеспечения защиты участников информационного обмена от обмана, осуществляемого на основе имитации, т. е., например подделки шифртекста до прихода подлинного шифртекста, подмены (навязывании) ложной информации после прихода подлинного шифртекста.

Под аутентификацией информации понимается установление подлинности информации исключительно на основе внутренней структуры самой информации независимо от источника этой информации, установление законным получателем (возможно арбитром) факта, что полученная информация наиболее вероятно была передана законным отправителем (источником) и что она при этом не заменена и не искажена.

Любые преднамеренные и случайные попытки искажений информации обнаруживаются с определенной вероятностью. Наиболее полно проблема аутентичности проявляется в вычислительных сетях, где можно выделить следующие ее виды:

Аутентификация пользователя сети – установление подлинности личности пользователя сети, которому требуется доступ к защищаемой информации или необходимо подключиться к сети;

Аутентификация сети – установление подлинности сети, к которой получен доступ;

Аутентификация хранящихся массивов программ и данных – установление факта, что данный массив не был изменен в течение времени, когда он был вне посредственного контроля, а также решение вопросов об авторстве этого массива данных;

Аутентификация сообщений – установление подлинности содержания полученного по каналам связи сообщения и решение вопросов об авторстве сообщения.

Решение указанных задач возможно как с применением классических систем шифрования, так и систем с открытым ключом.

Криптографические методы защиты информации основаны на использовании криптографических систем, или шифров. Криптосистемы позволяют с высокой степенью надежности защитить информацию путем ее специального преобразования. В криптопреобразовании используется один или несколько секретных параметров, неизвестных злоумышленнику, на чем и основана стойкость криптосистем.

Криптосистемы подразделяются на симметричные и несимметричные. В симметричных системах преобразование (шифрование) сообщения и обратное преобразование (дешифрование) выполняются с использованием одного и того же секретного ключа, которым сообща владеют отправитель и получатель сообщения. В несимметричных системах, или системах с открытым ключом, каждый пользователь имеет свою ключевую пару, состоящую из ключа шифрования и ключа дешифрования (открытого и секретного ключа), при этом открытый ключ известен остальным пользователям.

Основными методами являются шифрование, цифровая подпись и имитозащита сообщений.

Шифрование сообщений позволяет преобразовать исходное сообщение (открытый текст) к нечитаемому виду; результат преобразования называют шифротекстом. Злоумышленник без знания секретного ключа шифрования не имеет возможности дешифровать шифротекст. Для шифрования сообщений, как правило, используются симметричные криптосистемы.

Шифрование обеспечивает:

- *скрытие содержания сообщения*;
- *аутентификацию источника данных*: только владелец секретного ключа мог сформировать и отправить шифротекст; однако электронный документ не имеет при этом юридической значимости, так как возможен подлог со стороны получателя, также владеющего секретным ключом;

Цифровая подпись обеспечивает:

- *аутентификацию источника данных*: только владелец секретного несимметричного ключа мог сформировать цифровую подпись; получатель имеет только открытый ключ, на котором подпись может быть проверена, в том числе и независимой третьей стороной;
- *целостность сообщения*: злоумышленник не может целенаправленно изменить текст сообщения, поскольку это обнаружится при проверке цифровой подписи, включающей зашифрованную контрольную сумму сообщения; однако он имеет возможность случайно модифицировать шифротекст или навязать ранее переданный шифротекст.
- *юридическую значимость сообщения*: цифровая подпись по свойствам эквивалентна рукописной подписи по невозможности ее подделки, возможности проверки получателем документа и независимой третьей стороной (арбитром) и обеспечением аутентификации создателя подписи.

Имитозащита сообщений состоит в формировании контрольной суммы (имитовставки, кода аутентификации сообщения) по криптоалгоритму, добавляемой к сообщению. После этого сообщение с имитовставкой, как правило, шифруется по симметричному криптоалгоритму. Принципы формирования имитовставок (кодов аутентификации сообщений) подробно рассмотрены в аванпроекте "Разработка пакета программных средств обеспечения юридической значимости лицензий посредством цифровой подписи".

Имитозащита обеспечивает — целостность сообщения в соответствии со свойствами контрольной суммы.

Анализ существующих методов криптографических преобразований (034)

В настоящее время широкое применение нашли как симметричные, так и несимметричные криптосистемы.

Симметричные системы используются в основном для шифрования, а также для выработки криптографических контрольных сумм (имитовставки, хеш-функции). По способу использования средств шифрования информации обычно различают поточное и блочное симметричное шифрование. При поточном шифровании каждый символ исходного текста преобразуется независимо от других, что позволяет осуществлять шифрование одновременно с передачей данных по каналу связи. При блочном шифровании исходный текст преобразуется поблочно, причем преобразование символов в пределах блока является взаимозависимым.

Известно большое число алгоритмов блочного шифрования, в том числе принятых в качестве национальных стандартов. Наиболее известен американский алгоритм DES.

Шифрование сообщений осуществляется на абонентском или канальном уровне. Средства шифрования реализуются программно, аппаратно-программно или аппаратно.

Разработки в области канального шифрования ведутся в основном в странах НАТО. Среди фирм, изготавливающих подобное оборудование, наиболее известными являются: CyLink, Fredericks, Harris, GTE, E-Systems (США), Newbridge Microsystems (Канада), Siemens, Telefunken, Tele Security Timman (Германия), Philips USFA (Нидерланды), Cryptech Belgie (Бельгия), Plessy, Racal, Corros, Marconi (Великобритания).

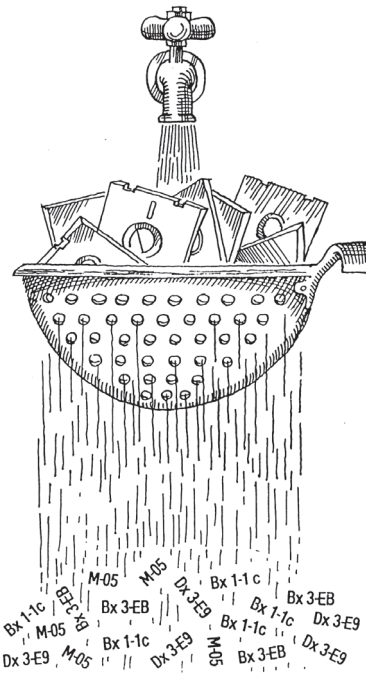
Интересным с точки зрения перспектив развития средств канального шифрования является предложенный фирмой Newbridge Microsystems (Канада) процессор CA20CO3A для шифрования данных по стандарту DES. Ключ хранится в энергонезависимой постоянной памяти, не имеющей доступа извне. Предлагаются версии процессора с тактовыми частотами 2,5 и 5 МГц.

Наиболее важными характеристиками средств шифрования, работающих на канальном уровне, являются:

- скорость шифрования;
- используемый алгоритм;
- режим работы;
- тип интерфейса;
- возможность работы в сетях с коммутацией пакетов X.25;
- тип возможных к использованию модемов;
- протоколы обмена ключевой информацией;
- способ ввода ключей;
- реализация функций обратного вызова, электронной подписи и др.

В основном скорости шифрования равны 64 Кбит/с для синхронного режима и 19,2 Кбит/с для асинхронного. Этого вполне достаточно для работы по выделенным телефонным линиям, но совершенно не приемлемо для обмена зашифрованной информацией по оптоволоконным линиям связи.

Для таких приложений могут подойти только высокоскоростные шифраторы CIDEC-HS, CIDEC-HSi, и CIDEC-VHS фирмы Cylink — мирового лидера в производстве средств канального шифрования. Устройство FX-709 также обеспечивает высокую скорость работы, но является мостом для соединения сетей Ethernet через интерфейсы RS-422 и RS-449.



Так выглядит процесс канального шифрования...

Для канального шифрования, как правило, используются потоковые шифры. Главным их достоинством является отсутствие размножения ошибок и высокая скорость. Единственным стандартным методом генерирования последовательностей для поточного шифрования остается метод, применяемый в стандарте шифрования данных DES в режиме обратной связи от выхода. Поэтому многие производители разрабатывают собственные алгоритмы, например фирма British Telecom реализовала в своих приборах B-CRYPT собственный секретный алгоритм B-152.

Пример

Программа аттестации коммерческих средств защиты связи CCEP (Commercial COMSEC endorsement program) Агентства национальной безопасности (АНБ) США предусматривает выдачу секретных криптоалгоритмов некоторым фирмам-изготовителям интегральных микросхем США для использования их только в США. Первый такой алгоритм был реализован фирмой Harris Semiconductor в ее криптографическом кристалле с интегральными микросхемами HS3447 Cipher.

Шифраторы, работающие на низких скоростях, обычно совмещают с модемами (STM-9600, Glo-Warm, Mesa 432i). Для средне- и высокоскоростных шифраторов изготовители обеспечивают совместимость с протоколами V.35, RS-449/422, RS-232 и X.21. Определенная группа приборов ориентирована на применение в узлах и конечных пунктах сетей с коммутацией пакетов X.25 (Datacriptor 64, Secure X.25L, Secure X.25H, Telecript-Dat, CD225, KryptoGuard).

Управление ключами — принципиально важный вопрос в любой криптосистеме. Большинство канальных шифраторов американского производства ориентировано на иерархический метод распределения ключей, описываемый национальным стандартом ANSI X9.17. В коммерческом секторе получают распространение криптосистемы с открытым распределением ключей. Например, фирма Cylink помимо реализации ANSI X9.17 имеет собственную запатентованную систему автоматического распределения ключей SEEK.

Ввод ключей в шифраторы может выполняться вручную с приборной панели, при помощи специальных карт либо дистанционно. Шифратором Glo-Warm можно управлять с сервера или рабочих станций; он имеет дополнительный внешний модуль дистанционного доступа.

Фирма Airtech, одна из первых начавшая производство стандартных встраиваемых блоков шифрования Rambutan, применяет магнитные карты для ввода ключей в канальные шифраторы. Фирма British Telecom выпускает карточку шифрования Lector 3000 для "дорожной" ЭВМ Toshiba TS 200/100 в версии с блоком Rambutan. Блок Rambutan разработан Группой безопасности связи и электронных средств CESG (Communications Electronics Security Group) Правительственного Управления связи Великобритании GCHQ (Government Communications Headquarters) специально для встраивания в аппаратуру, предназначенную для обработки и передачи важной правительственной информации, включающей и информацию с грифом "конфиденциально".

Интересно

Шифраторы фирмы Cylink имеют клавиатуру для ввода ключей и могут передавать сигналы тревоги и состояния прибора. Дистанционная система управления сетью CNMS (Cylink Network Management System) фирмы Cylink может контролировать до 256 шифраторов CIDECHSi из одного центрального пункта.

Несимметричные криптосистемы используются для формирования цифровой подписи и шифрования (формирования) симметричных ключей при их рассылке по каналам связи. Среди протоколов распределения ключей на практике используется метод Диффи-Хеллмана и метод цифрового конверта. Среди методов цифровой подписи наибольшее применение нашли RSA-подобные алгоритмы и алгоритмы на основе метода Эль-Гамаля, стандартизованные в ряде стран. Наиболее перспективным представляется использование усовершенствованного метода цифровой подписи Эль-Гамаля, который в последние годы стандартизован в США и России.

Защита данных при передаче по каналам связи ИС (030)

Подсистема связи считается наиболее уязвимой подсистемой ИС, поэтому следует уделить особое внимание вопросам ее защиты.

Такая защита осуществляется:

1. ***С целью защиты информации при передаче единичных сообщений (пакетов), которые могут стать объектами пассивных и активных вторжений.*** При пассивных вторжениях пользователи, не имеющие полномочий, лишь наблюдают за сообщениями, передаваемыми по линиям вязи, не изменяя этих сообщений. При активных вторжениях регулярные сообщения могут быть удалены, модифицированы, отсрочены, перенаправлены, защищены повторно или искажены. Возникающие при этом проблемы обусловлены непредвиденными ситуациями, аппаратными сбоями, помехами в линиях связи, программными ошибками и т.п.

2. ***Для обеспечения защиты и секретности операций, выполняемых над сообщениями при передаче по вычислительной сети.*** Объектами вторжений и источниками труд-

ностей в этом случае являются проблемы организации связи между двумя и более пользователями, протоколы передачи, устройства передачи и программное обеспечение систем передачи и т.д. Механизмы, обеспечивающие защиту операций в вычислительной сети, проектируются так, чтобы гарантировать целостность и защиту данных при передаче по сети.

Обеспечение конфиденциальности сообщения — одна из функций защиты от несанкционированного просмотра содержимого сообщения, гарантирующая его скрытность.

Обеспечение целостности — функция защиты от несанкционированных или случайных модификаций, гарантирующая правильность передачи содержимого сообщения.

Для защиты отдельных сообщений эти функции можно использовать как совместно интегрированно, так и раздельно.

Подлинность сообщения

Можно обеспечивать различными способами, не прибегая к его шифрованию. Такой подход пригоден во многих случаях, когда целостность данных играет исключительно важную роль, а конфиденциальность не требуется. Он используется при реализации финансовых операций и распределении открытых ключей между объектами сети. Широко распространены следующие ***методы обеспечения подлинности сообщения***:

- добавление к сообщению кода подлинности сообщения MAC (Message Authentical Code) или зашифрованной контрольной суммы;
- введение цифровых сигнатур.

Однако часто при передаче данных требуется гарантировать также конфиденциальность и целостность. В противоположность распространенному мнению оказывается, что использование криптографических систем для обеспечения конфиденциальности не всегда достаточно эффективно, например при защите от модификации сообщений.

Возможны случаи, когда целостность системы, использующей криптографическую защиту, может подвергаться опасности вторжения, если криптографическая система разрушена. Существуют также ситуации, когда криптографическая система, используемая для обеспечения конфиденциальности, создает также адекватную защиту целостности сообщений.

Принципы организации процедур подтверждения подлинности (034)

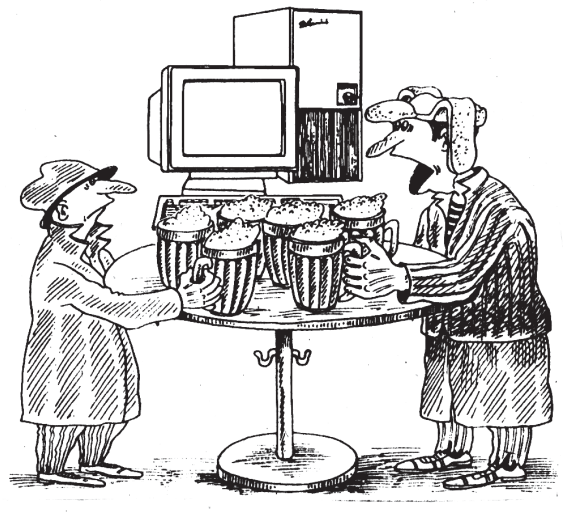
Большинство методов подтверждения подлинности получаемых зашифрованных сообщений должно использовать определенную избыточность исходного текста сообщения. Эта дополнительная информация должна быть известна получателю, и только после ее проверки можно сделать вывод о правильности переданного сообщения.

Избыточность может быть обеспечена разными способами. Например, можно воспользоваться избыточностью естественного языка, которая с трудом поддается автоматической проверке, но очевидна человеку. Другие типы избыточности, использующие контрольные цифры (например, номер банковского счета) значительно проще проверить.

Если не удается выбрать подходящий способ обеспечения избыточности, то отправителю и получателю достаточно договориться о добавлении в текст сообщения некоторой легко проверяемой дополнительной информации (до его шифрования).

Избыточность вводится на различных уровнях протокола вычислительной сети: на канальном — для контроля ошибок, на физическом (если используется шифрование) — для реализации проверки со стороны получателя. Поскольку такая проверка становится частью протокола передачи данных, это избавляет прикладной процесс от необходимости проверять избыточность.

Очевидно, чем больше избыточность исходного текста, тем проще получателю проверить подлинность сообщения и тем сложнее нарушителю модифицировать сообщение. Увеличения избыточности можно достичь, используя несколько ключей для шифрования и один ключ для дешифрования. Такой подход приводит к концепции истинной подлинности. А она обеспечивается такой системой шифрования, в которой знание ряда верных криптограмм не позволяет выявить истин-



Я гарантирую конфиденциальность, достоверность и подлинность своего сообщения...

ных шифрованных сообщений. Это означает, что злоумышленнику не остается ничего другого, как действовать наугад, а такой тактике легко воспрепятствовать, формируя очень большое число криптограмм, превышающее число правильных сообщений. Это еще раз подчеркивает значение избыточности исходного текста.

Многие криптосистемы обладают этим свойством, и истинная подлинность всегда достижима, хотя требуемое число ключей достаточно велико. Тем не менее следует оценить вероятность того, что случайная криптограмма окажется истинной. Примем за аксиому, что можно распознать содержимое сообщения. Следующая предпосылка состоит в том, что злоумышленник знает или может с большой вероятностью угадать исходный текст или его часть; такая ситуация зачастую вполне реальна. Затем его задача состоит в том, чтобы изменить исходный текст нужным образом, чтобы получатель восстановил в результате дешифрования измененный текст.

Защита целостности сообщений (734)

Побитовое шифрование потока данных

Такие системы шифрования наиболее уязвимы для тех вторжений, целью которых является изменение исходного текста. Если исходный текст частично известен злоумышленнику, модификация битов текста реализуется довольно просто, путем инвертирования битов шифрованного текста в тех местах, где требуется инверсия битов исходного. Такая модификация вполне реальна над финансовым сообщением, включающим, например, номиналы, число и номер купюр.

Если сообщение содержит лишь несколько контрольных знаков, они могут быть также изменены, поскольку все биты, участвующие в вычислении этих знаков, известны. Это оказывается возможным независимо от вида функции проверки избыточности (линейная или нелинейная).

Конечно, злоумышленнику необходимо знать эту функцию, и он может ее знать, поскольку проверочная функция не является секретной. Это означает, что шифрованные контрольные знаки, используемые в обычных протоколах передачи по линиям связи — символ контроля блока BCC (Block Check Character) и контроль циклическим избыточным кодом CRC (Cyclic Redundancy Check), не могут помочь получателю выявить манипуляции с сообщением, поскольку злоумышленник может легко вычислить их значения.

Подтверждение подлинности сообщения в таких системах требует специального механизма с засекреченными элементами, например кодом подлинности MAC (Message Authentication Code).

Побитовое шифрование потока с обратной связью по шифрованию

Для многих реализаций таких систем характерно явление непрерывного распространения ошибки, которое означает, что злоумышленник не в состоянии контролировать исходный текст, который будет восстанавливаться после умышленного изменения хотя бы одного бита. Исключение составляет ситуация, когда изменяемым является последний бит сообщения. Все виды контроля на избыточность будут работать как средства выявления ложных сообщений.

В других случаях возможно ограниченное распространение ошибки, например в пределах 64 бит в случае DES-алгоритма. Пока выполняется контроль по избыточности, который может выявить изменения по крайней мере в каждом 64-м бите, например с использованием символа контроля блока, то этого достаточно, поскольку злоумышленнику ничего не остается, кроме случайного угадывания.

Кстати

Существуют реализации, когда распространение ошибки не выходит за пределы одного бита. Не зная, как бит обратной связи влияет на дешифрование следующего бита, злоумышленник считает, что события "бит изменен" и "бит не изменен" имеют одинаковую вероятность (50%). Если в конце сообщения используется символ контроля блока, то злоумышленник может модифицировать его. Влияние обратной связи и модификации символа контроля блока на последующий блок одинаково и составляет по-прежнему 50%. Каждое изменение бита в одном или нескольких символах уменьшает эффективность успешного контроля на 50%.

Контроль с помощью циклического избыточного кода CRC или другого нелинейного метода, когда изменение одного бита влияет на несколько контрольных символов, создает для злоумышленника неблагоприятную ситуацию. В этом случае лучшей стратегией для злоумышленника было бы выявить те изменения, которые затрагивают лишь ограниченное число битов избыточного кода CRC.

DES-алгоритм в режиме 8-битового шифрования с обратной связью обладает теми же свойствами, что и в режиме побитового шифрования. Возможное, но вряд ли реализуемое 64-битовое шифрование с ОС имеет существенно иные свойства. Поскольку в этом случае побитовое шифрование распространяется на каждый 64-битовый блок, возможны манипуляции на уровне блока. Вставка или удаление блока могут быть выявлены. При известном исходном тексте можно выполнить изменение последнего блока, содержащего значения контрольных функций (символа контроля блока BBC

или циклического избыточного кода CRC), чтобы изменить значение контрольной функции. Сложение блоков по модулю 2 или добавление символа контроля блока не изменяют значения контрольной функции, если злоумышленник только переставляет блоки сообщения.

Побитовое шифрование с обратной связью по исходному тексту

Распространение вносимых в этом случае ошибок зависит от того, как биты сообщения влияют на работу генератора случайных чисел. Если этому влиянию подвергается только следующий бит, то вероятность правильного дешифрования уменьшается на 50% после каждого неправильного дешифрованного бита. Таким образом, дешифрование будет правильным только при условии, что никакие ошибки не вводятся. Это означает, что злоумышленник не в состоянии контролировать в полной мере все изменения, которые он вводит, и это, конечно, справедливо по отношению к модификации контрольных символов. Даже при использовании простейшей контрольной функции символа контроля блока — он будет иметь 50%-й шанс на успех. Использование более сложных функций контроля существенно снижает эффективность вторжения.

Однако весьма возможно, что такие системы имеют более широкую область распространения ошибки (и даже неограниченную). Если существуют проверочные функции для исходного текста, то введение в него нераспознаваемых изменений невозможно.

Поблочное шифрование потока данных

Нелинейные свойства процедур поблочного шифрования не позволяют злоумышленнику модифицировать блок исходного текста (байт или символ), даже если ему известно само исходное сообщение. Поскольку изменения исходного текста в результате поблочного шифрования предсказать невозможно, то злоумышленник не знает, как изменятся контрольные цифры, но даже если он знает, то не может осуществить желанных изменений. В результате такие системы обеспечивают высокую степень защиты от модификаций.

Поблочное шифрование потока с обратной связью (OC)

Область распространения ошибки составляет по меньшей мере следующий блок, а во многих системах и значительно больше. Степень защиты от возможных модификаций выше, чем в предыдущем случае.

Шифрование блоками

Область распространения ошибки ограничена размерами блока шифрованного текста, однако предвидеть эффекты изменений внутри блока невозможно. Тем не менее независимость блоков позволяет проводить манипуляции на уровне блока. Для DES-алгоритма это означает, что вполне реальны удаление или вставка 8-символьных блоков, изменение порядка их следования, причем без нарушения процедуры дешифрования. Могут быть вставлены даже блоки из других шифрованных сообщений, если используется одинаковый ключ шифрования.

Кстати

Многие функции контроля избыточности не могут выявить изменений такого рода. Например, использование символа контроля блока не позволяет выявить изменений порядка следования или двойные вставки, если последний блок, который содержит символы контроля блока, не затрагивается. В то же время типовые функции, которые зависят от положения проверяемых символов внутри сообщения (например, контроль циклическим избыточным кодом CRC), будут выявлять вставки, удаления и изменения следования блоков.

Шифрование блоками с обратной связью

В общем случае, когда обратная связь выполняет функцию ключа шифрования, изменения внутри шифрованного блока приводит к непредсказуемому изменению двух блоков исходного текста. Вставка или удаление влияют только на модифицируемый, однако этот результат непредсказуем. Все виды контроля избыточности в пределах блока эффективны.

В случае DES-алгоритма в режиме поблочного шифрования с ОС блок, используемый в ОС, добавляется по модулю 2 к следующему блоку исходного текста. Если после дешифрования изменить некоторые биты шифрованного блока, это может привести к модификации следующего блока. Если блок, в который вносятся искажения, используется для контроля избыточности, то он будет противостоять вторжению благодаря локализации и нераспространению ошибки. В свою очередь защита от модификаций на уровне самого блока значительно слабее.

Системы, использующие в обратной связи исходный текст, могут вызывать эффект неограниченного распространения ошибки, и, следовательно, применение контроля избыточности целесообразно для всех методов. Вполне достаточно для такого контроля завершения сообщения фиксированной константой.

Подтверждение подлинности сообщений

Вхождение пользователя в вычислительную систему естественно рассматривать как начало сеанса работы с терминалом и сопроводить его выполнением процедуры подтверждения подлинности. Такая процедура связана с подтверждением подлинности пользователя,

а не его сообщений. В сетях связи, наоборот, более важную роль играют сообщения: субъекты сети обмениваются сообщениями, и верификация источника и содержимого сообщения должна быть выполнена при получении каждого нового сообщения. Соответствующая функция защиты называется ***подтверждением подлинности сообщения***. Эта функция должна подтвердить следующие факты:

1. Сообщение исходит от санкционированного отправителя.
2. Содержание сообщения при передаче не изменялось.
3. Сообщение доставлено по адресу.
4. Аналогичное сообщение ранее не поступало.
5. Порядок получения сообщений соответствует порядку отправления.

В случае конфликтной ситуации третье лицо (посредник) должно удостоверить, что действительно сообщение послано одним санкционированным субъектом сети другому.

Известны три метода подтверждения подлинности сообщений с использованием:

- функций подтверждения подлинности;
- механизмов симметричного шифрования;
- механизмов шифрования с открытым ключом.

Защита потока сообщений

До сих пор рассматривалась только защита одиночных сообщений при передаче по сети, но обычно же между субъектами сети передается большое число сообщений и в течение длительного периода.

Основной ключ шифрования многократно используется при передаче сообщений. Это позволяет злоумышленнику задержать сообщения, удалить, подменить или повторить их. Подтверждение подлинности на уровне сообщений не обеспечивает защиты от таких действий, поскольку само сообщение при этом не изменяется. Тем не менее существуют различные методы для защиты от подобных вторжений.

Нумерация сообщений

Сопровождая каждое сообщение номером и включив его в содержание самого сообщения, а следовательно, и зашифровав, можно быть уверенным, что сообщение не является подменой. Такой номер должен быть связан с неким счетчиком, диапазон которого должен превышать время жизни ключа шифрования. Оборудование каналов связи должно обеспечивать обмен сообщениями в масштабе времени, близком к реальному, так, чтобы не нарушался порядок отправления и приема сообщений. Контроль номеров поступающих сообщений позволяет выявить вставки и удаления сообщений сразу после их приема. Контроль номеров поступающих сообщений позволяет выявить вставки и удаления сообщений сразу после прихода следующего сообщения.

Недостаток этой процедуры носит чисто организационный характер: каждый объект сети должен иметь различные счетчики для каждого из взаимодействующих с ним объектов. Номера передаваемых на канальном уровне блоков данных, которые являются частью протокола передачи, не могут быть использованы для этих целей, поскольку эти номера обнуляются при каждом новом соединении с абонентом и, следовательно, не могут быть использованы для подтверждения подлинности, хотя и являются зашифрованными.

Отметка времени

Сопровождая каждое сообщение информацией о дате и времени, получатель может проверить их актуальность. Интервал и точность такой отметки должны быть выбраны так, чтобы можно было, с одной стороны, выделить ошибочные сообщения, например быстрые повторы, а с другой — учесть естественные запаздывания, свойственные каналам передачи.

Использование случайных чисел

При применении двусторонней связи в реальном времени предполагаемый получатель может предварить передачу намечаемого сообщения посылкой отправителю случайного числа. Отправитель помещает это число в зашифрованное сообщение так, чтобы получатель мог его проверить. Таким способом могут быть легко отбракованы ложные сообщения.

Защита от манипуляций над потоками сообщений

Может быть реализована путем включения дополнительной избыточной информации в виде номеров сообщений или отметок времени в шифрованном сообщении. Эта информация может быть естественной частью формата сообщения и по аналогии с основным содержанием должна быть защищена от возможных манипуляций. Некоторые криптографические функции не обеспечивают необходимой защиты от искажения содержания. Идеальная ситуация — построить криптографическую систему, которая имела бы удовлетворительную процедуру подтверждения подлинности при наличии естественной избыточности сообщения; в противном случае необходимо вводить в сообщение специальные несекретные метки для выявления манипуляций, что усложняет систему защиты. Некоторые криптографические функции не обеспечивают удовлет-

ворительной защиты без специальных секретов кодов подтверждения подлинности, которые должны представлять дополнительный механизм обработки исходного или шифрованного текста.

Наиболее распространенные классы криптографических функций оценены именно в этом аспекте. Выбрав правильную криптографическую систему, можно существенно упростить реализацию процедуры подтверждения подлинности сообщений. Если шифрование применяется на физическом уровне, то в протоколе линии передачи данных достаточно использовать функции проверки с нормальным распределением ошибки. Если шифрование применяется на более высоком уровне, то аналогичные проверочные функции можно легко реализовать в формате сообщения (прикладной уровень протокола передачи данных).

Обеспечение защиты в протоколах передачи файлов

В большинстве ИС протокол передачи файлов реализуется в виде утилиты, обеспечивающей ограниченную защиту, основанную на механизмах защиты файлов используемой операционной системы. В большинстве случаев такая защита основана на иерархии привилегий, т.е. пользователи (процессы) для получения доступа к отдельному файлу должны иметь определенные права на использование этого файла.

Утилита сетевой передачи файлов взаимодействует с локальной системой управления файлами, и, как правило, именно эта система реализует средства работы с файлами. Так, например, утилита передачи файлов использует ее возможности доступа к файлам.

Что касается подсистемы передачи файлов, то доступ к файлам — только одна из многих функций, которые требуют средств защиты. Для реализации механизмов управления доступом в спецификацию файла должны быть включены идентификаторы пользователей и их права. Использование этих компонентов требует осторожности, и они должны быть недоступны.

Служба защиты при передаче файлов контролирует присваивание величин элементам в наборах данных. Присваивание должно осуществляться в соответствии с правилами и требованиями защиты, логически связанными со стратегией подсистемы передачи файлов.

Подсистема передачи данных представляет интерес не только в связи с защитой данных (в этом аспекте все механизмы обеспечения безопасности связи важны и полезны), но и в связи с защитой всей управляющей информации (т.е. атрибутов защиты файлов) таким образом, чтобы путь передачи конфиденциальной информации обеспечивался требуемыми условиями защиты всей сети или открытой системы. При этом необходимо обеспечение надежности линий связи.

Параметры защиты для стандарта ISO-OSI

ISO-OSI— стандарт доступа и управления передачей файлов FTAM (File Transfer Access and Management) определяет все необходимые правила работы с файлами. В стандарт FTAM включены определения файла, файловой системы, режима, фазы обработки, описаны абстрактные модели операций с файлами, включающие в себя понятия пользователей и разработчиков функций обработки файлов, реальной и виртуальной файловых систем, содержащих описание атрибутов файлов, файловых операций, их примитивов и параметров; связи между параметрами и атрибутами файлов и, наконец, протокол передачи файлов.

Атрибуты файлов объединяются в группы. Ядро составляют атрибуты, необходимые всегда и во всех случаях. Группа атрибутов хранения крайне разнородна; она содержит набор атрибутов, необходимых для отдельных операций над файлами. ***Они представляют собой основу группы атрибутов защиты, которая содержит атрибуты следующего назначения:***

- **Управление доступом**. Набор атрибутов, задающих условия доступа к файлу; доступ к файлу разрешен, если выполняется хотя бы одно условие.
- **Шифрование**. Параметр используется для указания алгоритма шифрования при сохранении данных. (Файл передается в шифрованном виде, во время передачи файлов дешифрование не применяется.) В соответствии со стандартом FTAM шифрование может применяться только к неструктурированным двоичным файлам. Этот атрибут не может быть изменен.
- **Правильная квалификация**. Скалярный атрибут, содержащий информацию о правильном статусе файла и его использовании; этот атрибут устанавливается при создании файла, но не может быть изменен; поддержка этого атрибута зависит от способа защиты данных.
- **Подтверждение подлинности**. Скалярный атрибут, который указывает на подлинность информации, сформированной разработчиком операций обработки при создании подсистемы передачи файлов.
- **Пароль**. Векторный атрибут, каждый элемент которого содержит величину, связанную с одним из восьми элементов требуемого атрибута доступа. Эти величины устанавливаются в соответствии со значениями примитивов выборки и создания файлов. Атрибут используется при передаче паролей, списка возможностей или элементов шифрования с открытым ключом.
- **Частное использование**. Набор атрибутов, значения которых не определены в стандарте; они могут быть изменены во время существования файла.

Итак, множество функций в стандарте FTAM связано с защитой и управлением доступом. Группа атрибутов защиты, соответствующая стандарту FTAM, мо-

жет быть определена только в том случае, если указана группа атрибутов хранения. При этом возникает проблема согласования изменяемых атрибутов, когда один из них — основной, а остальные подчинены ему.

Желающие использовать защиту подсистемы передачи файлов, должны хорошо разбираться не только в атрибутах файлов, но и в абстрактных моделях операций обработки файлов, заданных в стандарте FTAM, поскольку они представляют собой специальные механизмы защиты файлов и их передачи, необходимые для формирования надежной основы для связи отправителя с получателем.

Элементы защиты стандарта FTAM

Ознакомимся с элементами стандарта FTAM, которые могут быть использованы для реализации защиты и безопасности при передаче файлов. Кроме постоянного набора атрибутов, для каждого отправителя имеются атрибуты по каждой выполняемой операции. Этот набор можно расширить для повышения эффективности защиты подсистемы передачи файлов.

Кстати

Функционирование подсистемы передачи файлов носит обычно асимметричный характер: отправитель — активная сторона, а получатель файла — пассивная. Поток данных в большинстве случаев бывает однонаправленным. Это необходимо учитывать при реализации защиты подсистемы передачи файлов. В стандартах ISO определены два типа передачи данных: надежная и исправимая. При обеспечении защиты необходимо тщательно изучать особенности операций обоих типов.

Фаза выбора файла начинается с запроса на передачу отдельного файла. Последний можно выбрать по имени или определенной комбинации атрибутов. Это означает, что в фазе выбора для управления доступом целесообразно воспользоваться некоторой специальной информацией.

В ряде случаев по отношению к некоторым файлам может быть применена операция изменения атрибутов. При выполнении этой весьма ответственной операции необходимо тщательно изучить вопросы защиты.

Функции защиты линий связи

Защита содержимого сообщений достигается шифрованием. Чтобы обеспечить необходимую гибкость и скорость, следует применять симметрические криптографические системы. Для DES-алгоритма рекомендуется использовать режим поблочного шифрования с обратной связью.

Целостность передаваемых сообщений обеспечивается либо криптографическими методами, либо с помощью некоторой контрольной функции. Существуют различные механизмы, основанные на совместном использовании генератора случайных чисел и криптографических преобразований. Вся необходимая для этих механизмов управляющая информация должна быть включена в список параметров пользователя в таблице защиты UST. Различные типы контрольных функций могут быть найдены в литературе: от простейших функций подтверждения подлинности, основанных на алгоритме с усечением до n битов, использующих 32-битовую контрольную сумму, до очень сложных функций, использующих 128-битовый контроль.

Защита от наблюдения за трафиком реализуется при использовании анонимных сетей, особенность которых состоит в том, что при установлении связи между двумя пользователями используются условные идентификаторы, называемые псевдонимами.

Оба механизма ориентированы на применение асимметричных (открытых) криптографических систем, что позволяет не вводить дополнительных параметров в таблицу защиты.

Механизм защиты в виде чистого канала реализуется путем использования двух уровней шифрования: секретное сообщение можно восстановить, используя регулярный секретный ключ защиты, но для доступа к самому сообщению требуется дополнительный ключ. При этом необходимы две согласованные криптографические системы, поэтому в таблицу защиты добавляется второй ключ защиты.

Для обеспечения целостности потока сообщений могут применяться различные механизмы: нумерация номеров сообщений, отметка времени или уникальные идентификаторы сообщений. Такие механизмы при использовании специального протокола могут гарантировать целостность и достоверность процедуры обмена сообщениями. Поэтому в таблицу защиты, где каждый пользователь имеет один вход для каждого соединения, должны быть включены элементы защиты от активных вторжений. Такими элементами могут быть последовательность номеров сообщений, отметка времени, идентификатор сообщения или некоторая их комбинация. Таким образом, ***таблица защиты должна содержать:***

- личный секретный ключ;
- вектор инициализации;
- второй секретный ключ;
- последовательность номеров сообщений;
- маркер отчета времени;
- идентификатор сообщения (запроса).

Защищенный обмен сообщениями (030)

В настоящее время конфиденциальность электронной переписки можно обеспечить несколькими способами. Все они опираются на мощные средства шифрования, идентификации и фиксации авторства для гарантии того, что отправляемые и получаемые сообщения соответствуют оригиналу и поступают действительно от указанных лиц.

Интересно

Трудно поверить, но большинство компаний не используют каких-либо средств шифрования и идентификации при передаче обычных сообщений электронной почты. Так, исследование Gartner Group относительно защищенного обмена сообщениями показывает, что в 2001 году только 10–15% корпоративных пользователей будут иметь защищенную электронную почту.

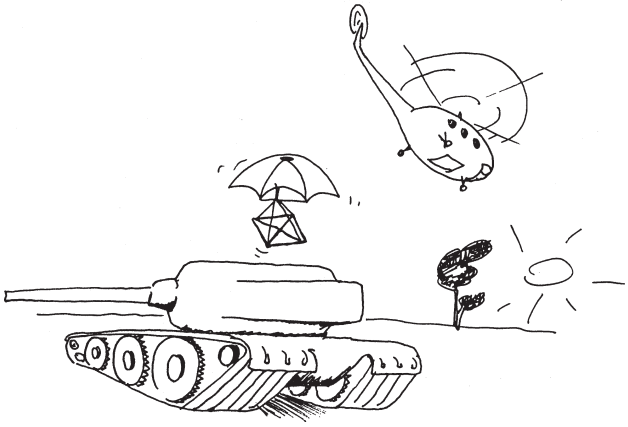
Только потому, что электронная почта передается одному или нескольким предопределенным получателям, многие пользователи полагают, что ее доставка так же защищена, как и телефонные звонки. Но если только вы не являетесь пользователем закрытой интерактивной службы типа CompuServe или AOL и не посылаете сообщений другим абонентам этой службы, вы не можете знать, каким путем сообщение попадет к адресату. Ввиду того, что сообщение электронной почты Internet проходит через многочисленные безымянные серверы прежде чем достигнуть конечного получателя, оно может быть перехвачено хакерами где-нибудь посреди маршрута.

Шифрование само по себе не обеспечивает адекватной защиты для сообщений, проходящих через Internet. Оно имеет мало смысла без идентификации. Тот факт, что вы получили сообщение от имени известного вам человека, еще не означает, что оно действительно было отправлено им.

Цифровая подпись и цифровой конверт (534)

Разработанный RSA в 1996 году, S/MIME стал весьма распространенным и широко признанным стандартом обмена сообщениями. Технология опирается на стандарт шифрования с открытыми ключами, и, таким образом, ее реализациям гарантирована совместимость на криптографическом уровне.

Двумя основными отличительными чертами S/MIME являются цифровая подпись и цифровой конверт. Цифровая подпись гарантирует, что сообщение не было изменено в процессе передачи. Кроме того, ее наличие не позволит отправителю отказаться от своего авторства.



Цифровой конверт...

Подпись представляет собой зашифрованное с помощью личного ключа отправителя резюме сообщения (само резюме вычисляется с использованием алгоритма хэширования). Для проверки целостности сообщения получатель расшифровывает подпись с помощью открытого ключа отправителя. Если получившееся резюме не совпадает с вычисленным, это означает, что сообщение было изменено в процессе передачи.

Однако цифровая подпись не гарантирует конфиденциальность сообщения. В S/MIME эту функцию выполняет цифровой конверт. Шифрование осуществляется с помощью симметричного алгоритма типа DES, Triple DES или RS2. Симметричный ключ шифруется с помощью открытого ключа получателя, а зашифрованное сообщение и ключ передаются вместе.

Помимо обеспечения защиты сообщения и гарантии его неизменения во время передачи S/MIME идентифицирует обладателя конкретного открытого ключа с помощью цифровых сертификатов X.509. Цифровой сертификат удостоверяет, что открытый ключ действительно принадлежит тому, от чьего имени он публикуется.

Кстати

Работая с S/MIME, пользователи могут выпускать свои собственные сертификаты, но, по словам Мэтью из RSA (который принимал участие в разработке S/MIME с самого начала), при отсутствии подтверждения от независимой стороны их полезность весьма ограничена. Цифровые сертификаты могут выпускать все, кто захочет, поэтому без посредничества независимой стороны для проверки и подтверждения вы не можете быть уверены, что эти сертификаты заслуживают доверия. Независимая сторона, например Verisign или GTE, может поручиться за достоверность сертификата.

Если компания намеревается выпускать свои собственные сертификаты, то она может воспользоваться продуктами (в частности, от Entrust Technologies) для создания инфраструктуры с открытыми ключами, способными не только выпускать сертификаты, но и управлять ключами на протяжении их жизненного цикла

Ваш знакомый PGP (534)

PGP, или Pretty Good Privacy, — один из тех примеров успеха, что у всех на устах. В 1991 году Фил Зиммерман, один из лучших умов в области криптографии, разработал программное обеспечение шифрования. Оказавшись в Internet, оно было загружено тысячами людей по всему миру. ***В настоящее время рассматривается протокол под названием Open PGP*** в контексте защиты электронной почты. Open PGP предусматривает несколько способов обеспечения целостности данных в сообщениях. Он поддерживает шифрование как с открытыми, так и с симметричными (секретными) ключами.

В модели с открытыми ключами данные шифруются с помощью однократного симметричного алгоритма, генерируемого отправителем. Этот однократный ключ тесно связан с сообщением, так как он используется только однажды. Затем он шифруется с помощью открытого ключа получателя и передается вместе с сообщением.

При получении сообщения Open PGP дешифрует однократный ключ, вложенный в сообщение, с помощью личного ключа получателя, имеющегося только у него. Затем Open PGP применяет дешифрованный однократный ключ для воссоздания полученного сообщения в первоначальном виде.

В модели с симметричными ключами пользователь может выбрать один из двух вариантов. Во-первых, сообщение можно зашифровать с помощью симметричного ключа, выводимого из пароля или другого общего секрета. Во-вторых, сообщение можно зашифровать по методу, напоминающему используемый в модели с открытыми ключами, когда однократный ключ шифруется с помощью симметричного алгоритма, выводимого из общего секрета.

Open PGP поддерживает также цифровые подписи, которые можно генерировать и вкладывать в сообщения. Сообщение и подпись шифруются затем с помощью однократного симметричного ключа, после чего однократный ключ шифруется с помощью открытого ключа и помещается перед всем зашифрованным блоком данных.

Крупные компании не торопятся с внедрением PGP, поскольку одна из его характерных особенностей — сеть доверительных отношений. Например, если пользователь А доверяет пользователю Б, а он, в свою очередь, доверяет пользователю В, то в соответствии с моделью доверительных отношений PGP пользователь В также доверяет пользователю А.

Защищенные каналы (634)

Часто межсетевые экраны используются еще и для создания защищенного от просмотра канала между несколькими сегментами сети intranet. Эта функция чрезвычайно удобна, поскольку позволяет очень эффективно использовать возможности Internet для корпоративных целей. Для создания таких каналов применяются специальные протоколы шифрования информации. При этом необходимо использовать достаточно быстрый алгоритм шифрования, так как объем передаваемой информации может быть большим, и медленные алгоритмы шифрования будут затруднять обмен сообщениями. Алгоритмы шифрования с открытым ключом обычно работают медленно, поэтому для шифрования больших потоков информации задействуются алгоритмы, в которых для шифрования и дешифрации используется одинаковый секретный ключ.

Сложность использования симметричного шифрования заключается в том, что отправитель и получатель сообщений должны знать одинаковый секретный ключ. Это означает, что передавать по сети такой ключ незашифрованным нельзя. Но передавать-то его нужно. Наиболее перспективное решение этой проблемы — шифровать секретные ключи по несимметричному алгоритму, а основной текст сообщения — по симметричному с применением секретных ключей. При этом снова возникает потребность в развитой системе сертификатов для передачи сообщений с помощью алгоритма открытых ключей. Причем в данном случае речь может идти не о сертификатах пользователей, а о сертификатах компьютеров, между которыми устанавливается защищенное от прослушивания соединение.

Защита потоков маршрутизатором (634)

Маршрутизаторы Advanced Remote Node (ARN), Access Stack Node 2 (ASN2) и BackBone Node (BN) имеют возможность управления доступом, протоколирования передаваемых потоков, шифрования данных при передаче пакетов и другие свойства, необходимые для построения межсетевого экрана. Их можно использовать для построения всей сети предприятия, что позволяет создать несколько уровней защиты для различных сегментов сети.

Маршрутизаторы управляются программным обеспечением Site Manager со специального выделенного

Маршрутизатор управляет...

компьютера — места администратора. Этот компьютер либо подключен напрямую к маршрутизатору через последовательный порт RS-232, либо находится в специальной административной сети, в которую нет входа извне, что позволяет на аппаратном уровне защитить консоль администратора, как наиболее уязвимое для нападения место.

Следует отметить, что средства защиты, такие как фильтрация пакетов, ведение протокола событий и маршрутизация, реализованы в маршрутизаторах на аппаратном уровне. Это позволяет максимально ускорить работу межсетевого экрана. А возможность установить приоритет на протокол или интерфейс либо перенаправить пакет позволяет администратору лучше контролировать распределение нагрузки на сетевую инфраструктуру.

Выбор средств защиты сообщений (534)

Сегодня S/MIME пользуется наибольшей популярностью среди разработчиков систем обмена сообщениями. Многие специализированные продукты имеют встроенную поддержку S/MIME, что упрощает построение защищенных систем обмена сообщениями.

Несмотря на то что RSA самостоятельно не разрабатывает пакетов для электронной почты, она имеет комплект инструментов, с помощью которого разработчики систем электронной почты могут встроить поддержку S/MIME в свои программные пакеты. Набор интерфейсов прикладного программирования RSA BSAFE S/MIME (формально известный как S/MAIL) позволяет включить алгоритмы шифрования и управления цифровыми сертификатами и ключами.

Встроенную поддержку S/MIME имеют Outlook Express и Outlook 98 компании Microsoft, а также компонент Messenger в Communicator от Netscape.

Worldtalk включила шифрование S/MIME в WorldSecure Server. Продукт представляет собой брандмауэр электронной почты с функциями централизованного администрирования правил защиты почты Internet в масштабах компании, фильтрации сорной почты по содержимому и сканирования на предмет наличия вирусов. Worldtalk также поддерживает S/MIME в своем WorldSecure Client, бесплатном подключаемом модуле для Exchange, Outlook, Lotus Notes и Eudora Pro (Qualcomm), благодаря которому пользователи могут шифровать и подписывать почту цифровым образом.

Кроме того, S/MIME поддерживается и клиентским программным обеспечением Express Mail компании OpenSoft. Продукт обеспечивает шифрование с ключом длиной до 2048 бит и совместим с цифровыми идентификаторами Verisign.

Продукты со встроенной поддержкой PGP не столь разнообразны, но тем не менее эта технология поддерживается некоторыми известными разработчиками. Так, Qualcomm включила PGP в четвертую версию популярного почтового клиента Internet Eudora Pro.

В текущей версии популярного пакета для коллективной работы GroupWise 5.5 Novell предпочла поддерживать как S/MIME, так и PGP. Пользователи GroupWise могут шифровать/дешифровать сообщения, ставить цифровые подписи, идентифицировать и фиксировать авторство с использованием S/MIME и инфраструктуры с открытыми ключами от Entrust. Аналогичные возможности они получают и используя PGP.

Выпустив PGP Desktop Security 6.0 в составе E-mail and Files 6.0 и PGP Desk 2.0 компания Network Associates упростила поддержку PGP. Являясь компонентом PGP Enterprise Security 3.0, PGP Desktop Security 6.0 содержит подключаемые почтовые модули для GroupWise, Outlook и других приложений электронной почты.

Совместимость средств защиты сообщений (534)

S/MIME и Open PGP — несовместимые спецификации. Большая часть пакетов электронной почты поддерживают либо один, либо другой протокол, но тенденция поддержки обоих все более набирает силу. Члены Internet Mail Consortium (IMC), отраслевой группы, целью которой является направление и поддержка усилий по распространению технологий электронной почты Internet, хотели бы иметь единый стандарт для защищенной электронной почты.

Кроме того, рабочая группа IETF, занимающаяся разработкой S/MIME, заявила, что она намеревается координировать свои усилия с рабочей группой Open PGP, так как эти две спецификации перекрываются в таких областях, как алгоритмы шифрования и структура MIME.

Интересно

Относительно совместимости с PGP Мэтью из RSA говорит следующее: "Я думаю, что мосты между S/MIME и PGP появятся задолго до того, как производители договорятся об общем стандарте для защищенного обмена сообщениями". Он добавляет, что общность в форматах сертификатов может послужить для этого хорошей исходной точкой, и его воодушевляет тот факт, что Network Associates начала двигаться в направлении совместимости с X.509. "Никто не может сказать, насколько компании готовы воспринять в качестве стандарта обе спецификации, но по крайней мере они хотели бы иметь возможность понимать PGP, так как он достаточно распространен", – говорит он.

Защита электронной почты (030)

Электронная почта (ЭП) в настоящее время широко используется благодаря своей дешевизне и оперативности. Вопросы защиты сообщений, обеспечения их целостности и подлинности, а иногда и конфиденциальности, важны даже при передаче личной почты. Возможность использования ЭП для передачи коммерческой и другой информации. содержащей конфиденциальные данные, всецело зависит от надежности услуг защиты, предоставляемых провайдерами для электронной почты или дополнительными средствами.

Рассмотрим этапы жизненного цикла ЭП и угрозы, связанные с возможностью модификации, подмена или доступа к содержанию ЭП. ЭП (рис. 14.2) состоит из краткого содержания письма (Subject), тела письма и прикрепленных (приатаченных) файлов. Каждый из перечисленных компонентов может отсутствовать. При формировании конверта почтовый клиент, например OUTLOOK EXPRESS, дополняет эти данные служебной информацией, такой как адрес отправителя и получателя, версия программы, данные о кодировке сообщений и приатаченных файлов и т.д. Сами компоненты письма помещаются в конверт в открытом виде. Например, если послано сообщение, которое в поле SUBJECT и в поле письма содержит слово TEST, то пересылаемое сообщение имеет вид:

Return-Path: <iit@vlink.kharkov.ua>

Received: from websrv (ns-pool23.vlink.kharkov.ua [212.82.204.55])

by stealth.vlink.kharkov.ua (8.11.1/8.11.0) with SMTP id f4I9FAV05708

for <iit@vlink.kharkov.ua>; Fri, 18 May 2001 12:15:10 +0300

Message-ID: <001101c0df7c$259cddb0$167dfea9@websrv>

From: "IIT" <iit@vlink.kharkov.ua>

To: <iit@vlink.kharkov.ua>

Subject: **TEST**

Date: Fri, 18 May 2001 12:22:44 +0300

MIME-Version: 1.0

Content-Type: text/plain;

charset="koi8-r"

X-Priority: 3

X-MSMail-Priority: Normal

X-Mailer: Microsoft Outlook Express 5.00.2919.6700

X-MimeOLE: Produced By Microsoft MimeOLE V5.00.2919.6700

Content-Transfer-Encoding: 8bit

X-MIME-Autoconverted: from quoted-printable to 8bit by stealth.vlink.kharkov.ua id f4I9FAV05708

TEST

РИС. 14.2. *Содержание ЭП.*

В этом тексте жирным выделена посланная информация. Как видно из этой иллюстрации, получив доступ к письму, мы легко прочитаем содержимое всех его полей. Получение же доступа к письму не представляет труда, существует много программ "слушалок", которые могут это выполнять, да и написание таких программ не требует высокой квалификации.

Используется несколько протоколов передачи и приема ЭП. Основными протоколами являются протоколы SMTP, POP3. Как показывает анализ этих протоколов, все части сообщения передаются даже без поля размера. Это означает, что возможно подмена отдельных частей письма, их удаление или вставка новой информации. Можно даже создавать новые письма, минуя почтовый клиент и "получать" письма, которые не отправлял сервер. Поэтому проблема защиты ЭП является актуальной.

Рассмотрим существующие средства защиты, встроенные в клиентские программы для работы с ЭП. Эти средства обеспечивают цифровую подпись (ЦП) и шифрование, но надежность этих средств очень мала, например, для шифрования используется симметричный алгоритм с длиной ключа 40 бит, что при современных возможностях вычислительных систем не достаточно.

Для подтверждения этого легко выполнить следующий эксперимент. Напишите циклический участок программы и измерьте время его выполнения для большого числа циклов. Зная это время для заданного числа циклов, можно вычислить требуемое время для количества циклов 240. Если учесть возможность распараллеливания этой задачи, вы убедитесь, что длина ключа в 40 бит не обеспечивает достаточного уровня защищенности даже при использовании прямого перебора. Современные методы криптоанализа симметричных алгоритмов позволяют уменьшить требуемое время на несколько порядков.

В последнее время большой популярностью пользуется пакет PGP (Pretty Good Privacy), на который не распространяются экспортные ограничения. Этот пакет встроен в почтовые программы неамериканского происхождения, например, The Bat!. Для ЦП этот пакет использует алгоритм RSA с ключами длиной до 4096 бит (начиная с версии 5.0) и симметричный алгоритм шифрования (IDEA) с длиной ключа 128 бит.

В чем же недостатки этой системы? Во-первых, она использует метод RSA, стойкость которого базируется на разложении произведения двух простых чисел на сомножители. Вопросы стойкости метода RSA исследовались многими авторами, например. Для решения этой проблемы появляются все более эффективные методы, например, метод решета общего числового поля GNFS (General Number Field Sieve), поэтому приходится все время увеличивать длину ключа. Увеличение длины ключа существенно увеличивает время, требуемое для ЦП, т.к. формирование ЦП сводится к выполнению операции модульного возведения в степень.

Несмотря на многочисленные методы ускорения этой операции, время выполнения остается существенным при обработке почтовых сообщений. Имеются и другие подходы к решению проблемы взлома RSA алгоритмов, основанные на изменении зашифрованного личного ключа и анализе подписи, сделанной измененным ключом. Поэтому применение встроенных средств защиты для передачи важной информации по ЭП невозможно.

Рассмотрим требования к системе защиты ЭП.

- Она должна обеспечивать все услуги безопасности, которые определяются ISO 7498-2 с помощью национальных криптографических алгоритмов, а именно: конфиденциальность информации, целостность информации, причастность, аутентификация, управление доступом.
- Она должна поддерживать работу с основными почтовыми клиентами, такими как OUTLOOK EXPRESS, MS OUTLOOK, The Bat!
- Она должна быть прозрачна для пользователя
- Она должна быть кроссплатформенной.

Заметим, что первое требование обязательно, все остальные – желательные.

Для построения такой системы проанализируем существующие способы и средства для построения систем защиты. В качестве криптографических алгоритмов будем использовать алгоритмы, принятые в качестве стандартов на Украине. Для ЦП используются алгоритмы ГОСТ 34.310-95, ГОСТ 34.311-95, для шифрования ГОСТ 28147-89.

Использование файлов

Структура системы с файловой защитой представлена на рис. 14.3.

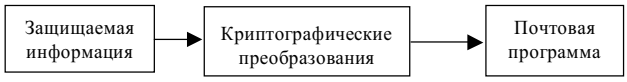


РИС. 14.3

Содержимое письма, тема и прикрепленные файлы подписываются и шифруются специальной программой, а затем прикрепляются к передаваемому письму. ***Достоинства этого способа:***

- на компьютере, подключенном в Интернет, информация в открытом виде не хранится, т.к. подготовку письма можно выполнять на любом другом компьютере;
- метод наиболее прост с точки зрения разработчика, т.к. не требуется взаимодействие программы для криптографических преобразований и почтового клиента.

Для простоты использования файлы для ЦП и шифрования могут располагаться на “Рабочем столе”, в этом случае их преобразование выполняется прямо с использованием контекстного пункта меню. Для добавления такого пункта достаточно в реестре для требуемых типов файлов (можно для всех типов) указать программу для ЦП и шифрования. ***Недостаток этого метода*** – не удовлетворяет требованию интеграции с почтовыми программами.

Построение системы ЭП с помощью Messaging Hook Provider

Схема преобразования информации с помощью Messaging Hook Provider представлена на рис. 14.4.

РИС. 14.4.

Данное средство позволяет перехватывать и выполнять обработку сообщений и прикрепленных файлов до и после их посылки транспортному провайдеру. На рис. 14.3 представлено прохождение почтового сообщения для случая посылки ЭП. При приеме ЭП пересылка информации выполняется в обратном направлении. Программно Messaging Hook Provider – это DLL специального вида, которая работает в адресном пространстве почтовой программы и получает сообщения в случае посылки почты или ее получении. Сервисы, заданные в DLL, регистрируются в Control Panel и далее их можно использовать для обработки сообщений. Messaging Hook Provider может обрабатывать любым образом сообщения до и после получения, в том числе выполнять их криптографические преобразования.

С точки зрения программиста аппарат использования Messaging Hook Provider несложный, но как показали исследования авторов, с помощью этого механизма можно подключаться только к некоторым почтовым клиентам. Такое подключение, например, возможно для MS OUTLOOK и невозможно для OUTLOOK EXPRESS. Поэтому далее будут рассмотрены другие методы, тем более, что для указанного почтового клиента есть более простой способ доступа к сообщениям – макросы.

Макросы являются и более универсальным способом, т.к. позволяют работать со всеми OFFICE продуктами, а не только с MS OUTLOOK.

Использование Макросов

Макросы позволяют обрабатывать события, связанные с отправкой почты (ItemSend) и ее приемом (NewMail). При обработке этих событий программист получает доступ к компонентам письма: предмет, тело письма и прикрепленные файлы. Эти компоненты могут быть преобразованы по заданным алгоритмам. Полученные макросы могут непосредственно использоваться при отправке почты из оффисных продуктов, например, Microsoft Word. Программа, которая использует макросы, прозрачна для пользователя, не сложна с точки зрения реализации.

Недостатки этого метода:

- Не решена проблема интеграции со всеми почтовыми клиентами, фактически макросы можно использовать только с MS OUTLOOK.
- Использование макросов всегда настораживает пользователя, т.к. макрос зачастую бывает источником вирусов.

Конечно, можно отключить проверку на наличие макросов, но в этом случае почтовая программа окажется беззащитной перед макросами – вирусами. Макрос может быть подписан, в этом случае операционная система (ОС) воспринимает его, как "свой" и не дает сообщения о наличии макроса. Для выполнения такой подписи необходимо использовать цифровой сертификат (сертификат разработчика) фирмы VeriSign. Перед выдачей такого сертификата сотрудники фирмы VeriSign должны связаться с фирмой Microsoft для подтверждения возможности выдачи. Такая процедура получения сертификата не всегда приемлема.

Использование WINDOWS HOOK

Хуки (HOOK) – это DLL, которые выполняются в адресном пространстве заданного или всех процессов. Позволяют выполнять определенные действия до и после выполнения оконной процедуры, при выполнении запросов к внешним устройствам, выборе пунктов меню и т.д. По сути позволяют преодолеть границы процесса. Достоинством метода является его универсальность, т.к. он работает с любым WIN32 приложением, ***недостатки метода:***

- необходимо либо перехватывать события данного класса для всех программ, что существенно замедляет выполнение всех приложений, либо необходимо инсталлировать программу защиты для каждого почтового клиента заново.
- Программисты, которые используют этот метод, должны быть готовы к регулярным переустановкам ОС. Метод "не устойчивый" на столько же, на сколько были не устойчивыми TSR приложения для DOS.

Использование сокетов (socket)

Сокет – это оконечное устройство канала связи (точка связи), через которую процесс может передавать или получать данные. Понятие сокета введено в ОС UNIX, имеются библиотеки для работы с соответствующими компонентами в большинстве визуальных средств, например, Visual C++, C++ Builder, ..., которые обеспечивают выполнение стандартных операций, связанных с соединением по заданным протоколам. Схема использования сокетов в системе защиты ЭП представлена на рис. 14.5.

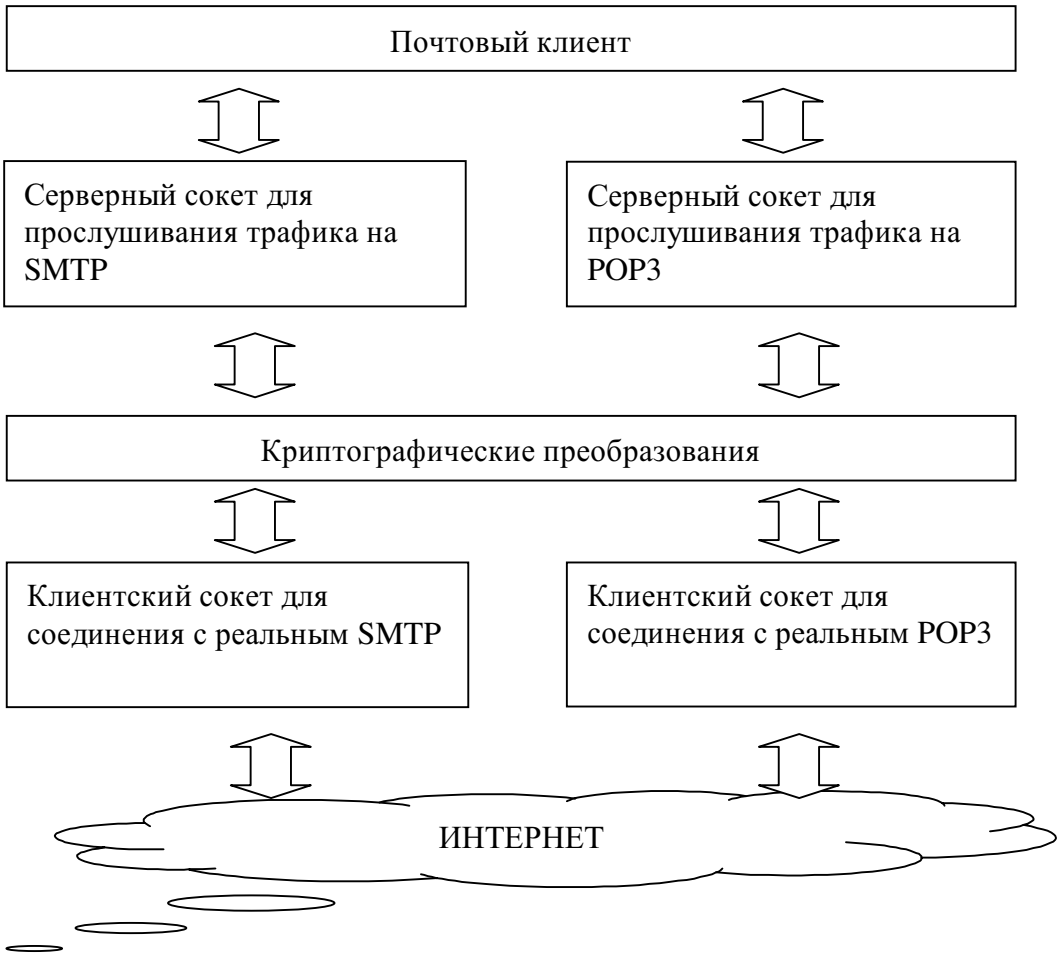


РИС.14.5

Наша цель внедриться т.е. стать посредникам передачи данных между почтовым клиентом и почтовым сервером, отмеченным на рис. 14.4 как ИНТЕРНЕТ. Для этого нам понадобится серверный сокет и клиентский сокет. С каждым сокетом связан порт, который он “слушает”. Для внедрения между почтовым клиентом и почтовым сервером достаточно почтовому клиенту задать вместо реальных IP адресов и портов почтового сервера IP адрес и порт нашего серверного сокета соответственно. Для увеличения надежности защиты будем располагать серверный сокет на том же компьютере что и почтовый клиент. В этом случае достаточно защитить только локальный компьютер, на котором установлены эти приложения. Сокет сервер нам нужен для прослушивание трафика от почтового клиента.

Полученные от почтового клиента данные подписываются шифруются и пересылаются клиентскому сокету, который связывается с реальным почтовым сервером.

Протокол передачи данных между реальным почтовым клиентом и сервером фактически не изменяется за счет того что команды передаются от Сокета сервера сокету клиенту без изменения.

Проблемы, которые необходимо решить программисту при использовании этого метода – все компоненты письма поступают на сокет пользователя во внутреннем представлении, поэтому необходимо исследовать способы кодировки компонентов письма, разработать функции для выделения и обработки отдельных компонентом и программ.

Заметим, что система на основе сокетов не зависит от почтового клиента, поэтому может быть легко интегрирована в любой почтовый клиент, который поддерживает протоколы POP3 и SMTP, и позволяет настраивать порты, используемые этими клиентами. К таким почтовым программам относятся, например, программы OUTLOOK EXPRESS, MS OUTLOOK, THE BAT! и многие другие. В связи с наличием средств

для поддержки работы с сокетами для большинства платформ, требование кросс платформенности может быть легко выполнено. Прозрачность с точки зрения пользователя также гарантируется, т.к. после запуска программы защиты она перехватывает все пакеты без дополнительных команд пользователя.

Здесь были рассмотрены основные особенности построения системы защиты ЭП с учетом требований прозрачности и многоплатформенности. Не изучены вопросы формирования и распространения ключей. С этой точки зрения данная система не отличается от аналогичных систем, в которых требуется распространение открытых ключей в режиме "каждый с каждым" или по заданному спи

Защита от фальшивых адресов (030)

От этого можно защититься с помощью использования шифрования для присоединения к письмам электронных подписей. Одним популярным методом является использование шифрования с открытыми ключами. Однонаправленная хэш-функция письма шифруется, используя секретный ключ отправителя.

Получатель использует открытый ключ отправителя для расшифровки хэш-функции и сравнивает его с хэш-функцией, рассчитанной по полученному сообщению. Это гарантирует, что сообщение на самом деле написано отправителем, и не было изменено в пути.

Правительство США требует использования алгоритма Secure Hash Algorithm (SHA) и Digital Signature Standard, там где это возможно. А самые популярные коммерческие программы используют алгоритмы RC2, RC4, или RC5 фирмы RSA.

Защита от перехвата (030)

От него можно защититься с помощью шифрования содержимого сообщения или канала, по которому он передается. Если канал связи зашифрован, то системные администраторы на обоих его концах все-таки могут читать или изменять сообщения. Было предложено много различных схем шифрования электронной почты, но ни одна из них не стала массовой.

Одним из самых популярных приложений является PGP. В прошлом использование PGP было проблематичным, так как в ней использовалось шифрование, подпадавшее под запрет на экспорт из США.

Коммерческая версия PGP включает в себя плагины для нескольких популярных почтовых программ, что делает ее особенно удобной для включения в письмо электронной подписи и шифрования письма клиентом. Последние версии PGP используют лицензированную версию алгоритма шифрования с открытыми ключами RSA.

Корректное использование электронной почты (030)

Все служащие должны использовать электронную почту так же, как и любое другое официальное средство организации. Из этого следует, что когда письмо посылается, как отправитель, так и получатель должен гарантировать, что взаимодействие между ними осуществляется согласно принятым правилам взаимодействия. Взаимодействие с помощью почты не должно быть неэтичным, не должно восприниматься как конфликтная ситуация, или содержать конфиденциальную информацию.

Защита электронных писем и почтовых систем (030)

Защита писем, почтовых серверов и программ должна соответствовать важности информации, передаваемой по сетям. Как правило, должно осуществляться централизованное управление сервисами электронной почты. Должна быть разработана политика, в которой указывался бы нужный уровень защиты.

Примеры политик безопасности для электронной почты (030)

Электронная почта предоставляется сотрудникам организации ***только для выполнения ими своих служебных обязанностей***. Использование ее в личных целях запрещено.

Конфиденциальная информация или информация, являющаяся собственностью организации, не может быть послана с помощью электронной почты.

Могут использоваться только ***утвержденные почтовые программы***.

Нельзя устанавливать ***анонимные ремэйлеры***.

Служащим запрещено использовать анонимные ремэйлеры.

Конфиденциальная информация или информация, являющаяся собственностью организации, не может быть послана с помощью электронной почты.

Если будет установлено, что сотрудник ***неправильно использует электронную почту*** с умыслом, он будет наказан.

Почтовая система должна обеспечивать ***только один внешний электронный адрес*** для каждого сотрудника. Этот адрес не должен содержать имени внутренней системы или должности.

Должен вестись ***локальный архив MIME-совместимых программ*** для просмотра специальных форматов и быть доступен для внутреннего использования.

Все электронные письма, создаваемые и хранимые на компьютерах организации, являются ***собственностью организации*** и не считаются персональными.

Организация оставляет за собой ***право получить доступ к электронной почте сотрудников***, если на то будут веские причины. Содержимое электронного письма не может быть раскрыто, кроме как с целью обеспечения безопасности или по требованию правоохранительных органов.

Пользователи не должны позволять кому-либо посылать письма, используя их идентификаторы. Это касается их начальников, секретарей, ассистентов или других сослуживцев.

Организация оставляет за собой право осуществлять ***наблюдение за почтовыми отправлениями сотрудников.*** Электронные письма могут быть прочитаны организацией даже если они были удалены и отправителем, и получателем. Такие сообщения могут использоваться для обоснования наказания.

Справочники электронных адресов сотрудников не могут быть сделаны доступными всем.

Если с помощью электронного письма должна быть послана конфиденциальная информация или информация, являющаяся собственностью организации, она ***должна быть зашифрована*** так, чтобы ее мог прочитать только тот, кому она предназначена, с использованием утвержденных в организации программ и алгоритмов.

Никто из посетителей, контрактников или временных служащих ***не имеет права использовать электронную почту*** организации.

Должно использоваться шифрование всей информации, классифицированной как критическая или коммерческая тайна, при передаче ее через открытые сети, такие как Internet.

Выходящие сообщения могут быть ***выборочно проверены***, чтобы гарантировать соблюдение политики.

Входящие письма должны ***проверяться на вирусы*** или другие РПС.

Почтовые сервера должны быть сконфигурированы так, чтобы ***отвергать письма***, адресованные не на компьютеры организации.

Журналы почтовых серверов должны проверяться на предмет ***выявления использования неутвержденных почтовых клиентов*** сотрудниками организации, и о таких случаях должно докладываться.

Почтовые клиенты должны быть сконфигуированы так, чтобы каждое сообщение ***подписывалось с помощью цифровой подписи*** отправителя.

Хранение электронных писем (030)

Официальные документы организации, передаваемые с помощью электронной почты, должны быть идентифицированы и должны администрироваться, защищаться и сопровождаться настолько долго, насколько это нужно для деятельности организации, аудита, юристов, или для других целей. Когда электронная почта — это единственный способ передачи официальных документов компании, то к ним применяются те же самые процедуры, как если бы они передавались на бумаге.

Для предотвращения случайного удаления писем, сотрудники должны направлять копии таких сообщений в официальный файл или архив. Должны храниться как входящие, так и выходящие сообщения с приложениями. Любое письмо, содержащее формальное разрешение или выражающие соглашение организации с другой организацией, должно копироваться в соответствующий файл(или должна делаться его печатная копия) для протоколируемости и аудита.

Период хранения всех писем определяется юристами. Если сообщения хранятся слишком долго, организация может вынуждена сделать такую информацию публичной по решению суда.

Несколько советов и рекомендаций (633)

Первое, о чем компания должна побеспокоиться, — это ***наличие в корпоративной системе обмена сообщениями базовых средств защиты***. По крайней мере вы должны быть уверены, что сообщение шифруется каждый раз, когда сотрудник нажимает кнопку Send на своем почтовом клиенте. Кроме того, немаловажное значение имеет ***возможность быстро дешифровать сообщение на почтовом сервере.***

Развертывание инфраструктуры с открытыми ключами имеет важное значение не только для организации защищенного обмена сообщениями, но и для создания защищенной системы идентификации в сети, и для предоставления пользователям прав доступа к базам данных, каталогам и другим сетевым компонентам.

Первым шагом в этом направлении является встроенная поддержка сертификатов в S/MIME и PGP. Она может послужить исходной точкой для развертывания полномасштабной инфраструктуры с открытыми ключами.

Защищенный обмен сообщениями, надежная идентификация и электронная коммерция невозможны без инфраструктуры с открытыми ключами (Public Key Infrastucture, PKI).

PKI — это не только создание цифровых сертификатов. Она служит для хранения огромного количества сертификатов и ключей, обеспечения резервирования и восстановления ключей, взаимной сертификации, ведения списков аннулированных сертификатов и автоматического обновления ключей и сертификатов после истечения срока их действия.

Интересно

"Защита сообщений электронной почты во многом аналогична шифрованию настольных файлов, – говорит Ян Карри, директор по продуктам в Entrust Technologies, лидере в области технологий для PKI. – Вы по-прежнему используете шифрование как с несимметричными, так и с симметричными ключами, но механизмы при этом совершенно иные".

Карри добавляет, что, хотя S/MIME поддерживает сертификаты X.509, а PGP развивается в направлении поддержки X.509, этого недостаточно. "S/MIME – это стандарт на формат данных, и он не дает никакой информации о том, откуда берутся пары ключей, как проверить сертификат по списку аннулированных сертификатов и как осуществляется взаимная сертификация. Это не PKI", – завершает он свою мысль.

S/MIME и PGP могут поддерживать сертификаты и даже хранить ограниченное их число, но создание PKI делает защиту и идентификацию куда более надежной. Этот факт признается даже RSA Data Security, творцом S/MIME.

"Я думаю, что люди еще не в полной мере оценили достоинства подобной идентификации, – говорит Тим Мэтью, директор по маркетингу в RSA. – При наличии надежной идентификации электронных документов вы можете отказаться от многих процессов, ранее осуществлявшихся исключительно с использованием бумаги".

Защита телефонных линий от прослушивания (630)

По заявлению Ф.Джонсона, специалиста по техническим каналам связи из Нью-Йорка, в американской практике для сбора коммерческой информации конкурентов телефон используется в семнадцати случаях из ста. И вероятно только финансовая проблема сдерживает поток любителей чужих тайн. Стоимость современных средств телефонного контроля, широко рекламируемых и предлагаемых в свободной продаже в западных магазинах, колеблется от десятка до нескольких сотен долларов. Установка же такой аппаратуры, как, впрочем, и ее эксплуатация, почти всегда настолько дороги, что доступны далеко не каждой фирме.

Факты

До середины 80-х годов телефонные переговоры в СССР контролировались только спецслужбами и правоохранительными органами. Как утверждал бывший глава КГБ СССР Вадим Бакатин, до августовского путча 1991 года 12-й отдел КГБ СССР прослушивал в Москве 300 абонентов, в основном иностранных граждан и преступников.

Контроль служебных переговоров велся и на объектах особого режима, но здесь уже следили не за конкретным человеком, а за утечкой секретной информации. В этом случае использовались специальные системы, работающие по ключевым словам и позволяющие прерывать или телефонный разговор, или отдельные фразы. При этом легко устанавливались номера абонентов-нарушителей режима.

Однако аппаратура для подобного контроля стоила очень дорого — порядка 200 тыс. руб. (по ценам 80-х годов) и применялась в основном на крупных объектах оборонной промышленности, в штабах воинских подразделений и в правительственных учреждениях.

В наше время прослушать телефонную линию стало простым и дешевым делом. Можно уверенно заявить о том, что если злоумышленник принял решение о “разработке” объекта, то первое, что он скорее всего сделает, это начнет контроль телефонных переговоров этого объекта. Злоумышленник без захода в помещение объекта при минимальных затратах и минимальном риске может осуществлять полный контроль за телефонными переговорами объекта.

В конце 80-х — начале 90-х годов на рынок, начала поступать западная техника для контроля телефонных каналов, которая теперь эффективно используется и в промышленном шпионаже. Так, при рассмотрении уголовного дела по факту вымогательства (рэкет) у одного из московских СП было выявлено, что преступники организовали телефонный контроль за руководством СП, службой безопасности, прослушивали все телефонные разговоры. При этом использовали портативные устройства, популярные среди детективов, контролирующих дельцов наркомафии. Стоимость таких устройств, имеющих радиотелефонный канал связи с подслушиваемой линией, около 200 тыс. дол. Способы подключения к телефонным линиям с целью снятия информации показаны на рисунках 14.6–14.10.

Полная инженерно-техническая защита телефонных переговоров, кроме простейших устройств (их цена 5–40 дол. за штуку), стоит сегодня от нескольких сотен тысяч до миллиона долларов. Обеспечение же только одного телефонного абонента аппаратурой специальной связи типа знаменитой “Кремлевки” обходилось в 80 тыс. руб. в год по ценам декабря 1991 г. Возможно, кто-то из предпринимателей до сих пор заблуждается, считая такие затраты непозволительной роскошью. Но как известно, скупой платит дважды...

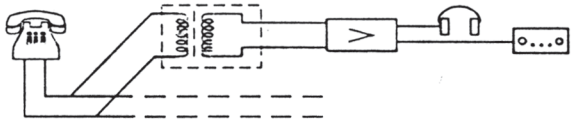


РИСУНОК 14.6. *Подключение к телефонной линии с помощью согласующего устройства.*

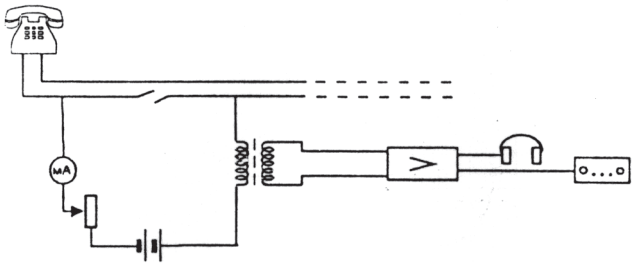


РИСУНОК 14.7А. *Подключение к телефонной линии с компенсацией напряжения.*

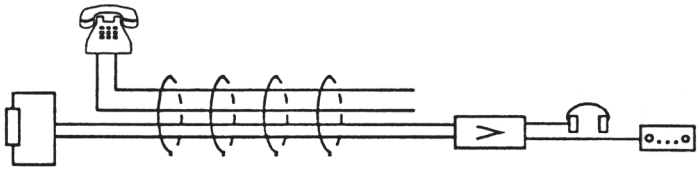


РИСУНОК 14.7Б. *Подслушивание за счет наводок.*

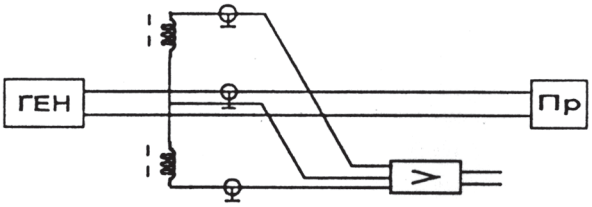


РИСУНОК 14.8. *Подключение к линии индукционного датчика.*

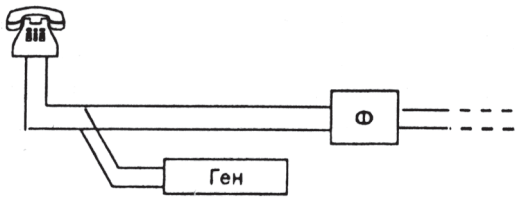


РИСУНОК 14.9. *Блок-схема высокочастотного "навязывания".*

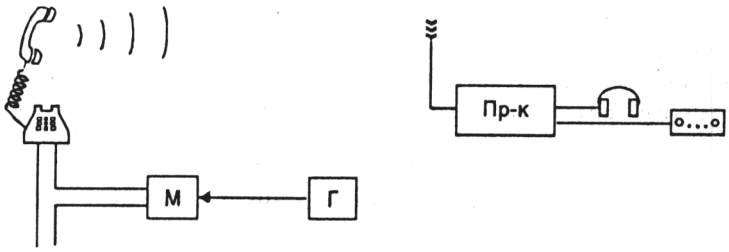


РИСУНОК 14.10. *Блок-схема телефонной радиозакладки.*

Работники одной из преуспевающих московских брокерских контор стали замечать, что все ее сделки срываются и переходят к конкурентам, работающим на одной бирже. С помощью сотрудников местной детективной службы коммерсантам удалось обнаружить не только наружное наблюдение, организованное конкурирующей фирмой, но и стандартные закладки с автоматической магнитной записью на некоторых телефонах брокеров фирмы. Стоимость такой закладки 200–400 дол., потери же брокерской конторы составили 20 млн. руб. в месяц.

Торги на бирже. На размышление брокерам — всего пять минут. Всем брокерам, кроме одного. Он получил информацию на час раньше других и за это время нашел выгодного заказчика, который смог предложить за товар самую высокую цену. Дело в том, что информацию эта брокерская контора похитила с АТС, к которой подключены все 15 телефонов биржи. Снимаются сведения и с факсов, которые работают на бирже круглосуточно. Так что к утру, к началу торгов, кто-то оказывается хозяином положения.

На Западе производство прослушивающих устройств составляет одну из основных статей дохода фирм, занимающихся этим специфическим видом бизнеса. К примеру, только фирма LEA (Lawentorcement associates, inc) представляет для потенциальных пользователей — правоохранительных органов и криминальных служб, частных лиц более 10 таких устройств разного назначения по цене от нескольких десятков до сотен тысяч долларов.

В СССР производством спецтехники по заказу КГБ, МВД, ГРУ занимались предприятия и научные институты Минрадиопрома и Минэлектронпрома. Отечественные специалисты считают, что советская продукция, как правило, не уступала по качеству зарубежным образцам, хотя на широкий рынок не попадала. Только в 1990 г. появились фирмы по продаже техники на открытом рынке в основном западного образца и за валюту. Одной из первых этим бизнесом занялась фирма "Valtex international comporation" (США), поставляющая в Россию — в основном для МВД — американскую спецтехнику.

На сегодняшний день на рынке представлены ***пять разновидностей доступной техники, предназначенной для защиты телефонных каналов:***

- криптографические системы защиты (для краткости скремблеры);
- анализаторы телефонных линий;
- односторонние маскираторы речи;
- средства пассивной защиты;
- постановщики активной заградительной помехи.

Факты

Спецслужбы имеют на вооружении аппаратуру, позволяющую прослушивать переговоры, ведущиеся по подземным линиям связи. Рассмотрим принцип ее действия на примере американской системы "Крот". С помощью специального индуктивного датчика, охватывающего кабель, снимается передаваемая по нему информация. Для установки датчика на кабель используются колодцы, через которые проходит кабель. Датчик в колодце укрепляется на кабеле и для затруднения обнаружения проталкивается в трубу, подводящую кабель к колодцу. С помощью закрепленного на кабеле датчика высокочастотный сигнал, несущий информацию о ведущихся по кабелю переговорах, записывается на магнитный диск специального магнитофона.

После заполнения диск заменяется новым. Запись с диска передается на установленные в помещениях спецслужб в зданиях посольств приборы демодуляции и прослушивания. В целях упрощения задачи поиска устройства "Крот" для замены диска оно снабжено сигнальной радиостанцией. Агент, проезжая или проходя в районе установки прибора-шпиона, запрашивает его с помощью своего портативного радиопередатчика, все ли в норме. Если никто не трогал, то оно передает соответствующий сигнал. В этом случае при благоприятных условиях агент заменяет диск в магнитофоне и работа устройства продолжается. Аппарат может записывать информацию, передаваемую одновременно по 60 телефонным каналам. Продолжительность непрерывной записи разговора на магнитофон составляет 115 ч. Такие устройства находили в Москве.

Более десяти аналогичных "Кротов" по просьбе сирийской стороны было снято нашими специалистами в Сирии. Там все подслушивающие устройства были закамуфлированы под местные предметы и заминированы на неизвлекаемость. Часть из них при попытке извлечения взорвалась. Для различных типов подземных кабелей разработаны разные подслушивающие устройства: для симметричных высокочастотных кабелей – устройства с индуктивными датчиками, для коаксиальных и низкочастотных кабелей – с системами непосредственного подключения и отвода малой части энергии для целей перехвата. Для кабелей, внутри которых поддерживалось повышенное давление воздуха, применяются устройства, исключающие его снижение, в результате чего предотвращается срабатывание специальной сигнализации. Некоторые приборы снабжаются радиостанциями для прямой передачи подслушанных разговоров в центр их обработки.

(Лысов А.В., Остапенко А.Н. "Промышленный шпионаж в России. Методы и средства.")

Наверное, читатель уже догадался, что от "чуткого уха" в наше время укрыться нельзя нигде. И все-таки, можно ли "перехитрить" технику и сохранить в тайне содержание переговоров? С уверенностью скажем "да", если вы начнете с выполнения следующих простых советов.

Прежде чем обратиться за помощью к частным детективам, постарайтесь ответить самому себе на несколько вопросов. Отнеситесь к этому заданию серьезно, что поможет вам в дальнейшем эффективно провести необходимые организационные и технические мероприятия, а может быть, излечит от излишней подозрительности. Итак, кто (государственная организация, фирма, частное лицо) может организовать прослушивание телефонных аппаратов в вашем офисе и с какой целью?

Интересно

Телефонный радиотранслятор

Телефонные закладки могут подключатся к любой точке телефонной линии и иметь неограниченный срок службы, так как питаются от телефонной сети. Эти изделия чрезвычайно популярны в среде промышленного шпионажа благодаря простоте и дешевизне (от 15 до 200$).

Большинство телефонных закладок представляют собой специальные радиозакладки. Они автоматически включаются при поднятии телефонной трубки и передают по радиоканалу телефонный разговор на пункт перехвата, где он может быть прослушан и записан.

Так как телефонный аппарат имеет свой микрофон и закладкам не нужен источник питания, их размеры могут быть миниатюрными.

Более совершенные, хотя и со значительно меньшей дальностью закладки выпускаются в виде конденсаторов, которые устанавливаются в самом телефонном аппарате или в розетке (ЛСТ-5К). Выпускаются также комбинированные системы обеспечивающие прослушивание и телефонов и помещений (ЛСТ-5-1). Интересное изделие предлагает фирма SIPE. Изделие ТК CRISTAL сделана в виде микрофона телефонного аппарата и может быть установлена в него за несколько секунд. Частота передатчика стабилизирована кварцем. Дальность действия 150 м.

(Лысов А.В., Остапенко А.Н. "Промышленный шпионаж в России. Методы и средства.")

За кем из ваших сотрудников может быть установлен телефонный контроль? Какая информация может интересовать ваших конкурентов? Какие телефонные аппараты могут находиться на контроле и в какое время? Проанализировав возможные ответы на поставленные вопросы можно сделать выводы, упрощающие задачу поиска канала утечки информации. Прежде всего, следует уделить серьезное внимание вашему офису. Поручайте выполнение ремонтных и строительных работ только тем фирмам, которым доверяете, но даже в этом случае обязательно организуйте контроль или охрану. Если вы подозреваете что была заложена подслушивающая аппаратура, проведите с помощью специалистов проверку помещений. Учтите, что стационарные закладки устанавливаются на том этапе, когда уже известно, где и как располагаются служебные помещения в будущем офисе (кабинет руководителя фирмы, секретаря, комната переговоров и т.д.). Основные способы подслушивания телефонных переговоров представлены на рисунке 14.11.

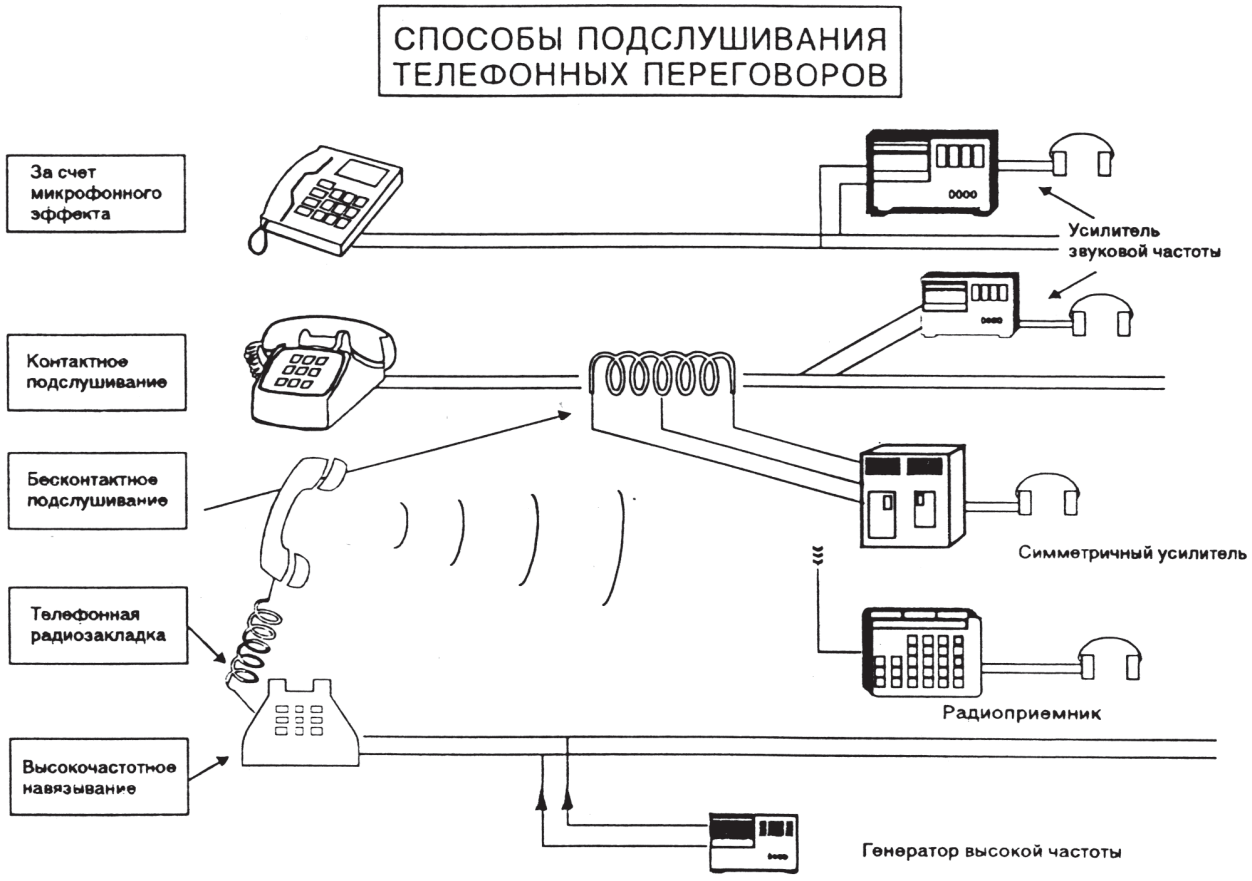


РИСУНОК 14.11. *Способы подслушивания телефонных переговоров.*

СКРЕМБЛЕРЫ

Надо знать

Работа таких систем делится на несколько этапов. На первом этапе речевое сообщение абонента обрабатывается по какому-либо алгоритму (кодируется) так, чтобы злоумышленник, перехвативший обработанный сигнал, не смог разобрать смысловое содержание исходного сообщения. Затем обработанный сигнал направляется в канал связи (в телефонную линию). На последнем этапе сигнал, полученный другим абонентом, преобразуется по обратному алгоритму (декодируется) в речевой сигнал с неизбежной потерей качества (рис. 7.8).

Принято считать, что скремблеры обеспечивают наивысшую степень защиты телефонных переговоров. Это действительно так, но только в том случае, если алгоритм кодирования-декодирования имеет достаточную криптостойкость. Аналоговые алгоритмы кодирования, которые используются в скремблерах ценой от 300 до 400$ за прибор, более просты и поэтому менее стойки, чем у систем с цифровой дискретизацией речи и последующим шифрованием. Но стоимость последних и выше как минимум в 3 раза.

К достоинствам криптографических систем следует отнести то, что защита происходит на всем протяжении линии связи. Кроме того, безразлично, какой аппаратурой перехвата пользуется злоумышленник. Все равно он не сможет в реальном масштабе времени декодировать полученную информацию, пока не расколет ключевую систему защиты и не создаст автоматический комплекс по перехвату.

(С. Е. Сталенков, Е. В. Шулика ЗАО НПЦ Фирма "НЕЛК")

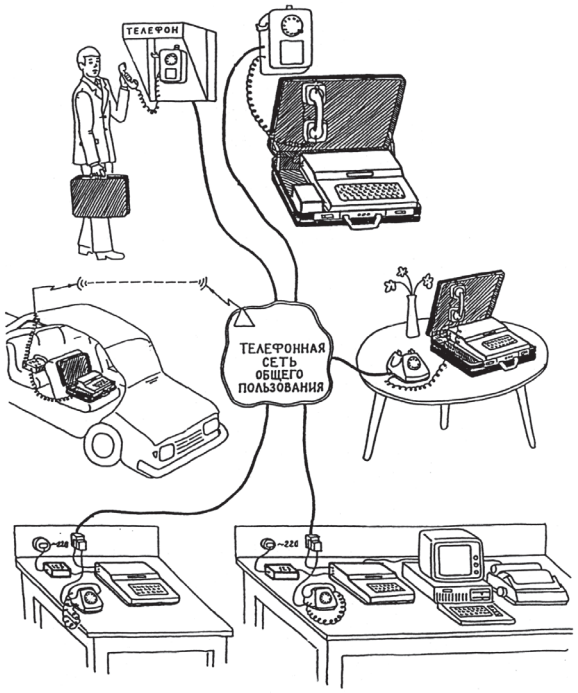


РИСУНОК 14.12. *Варианты использования средств шифрования.*

Необходимо, прежде всего, определить порядок ведения переговоров по телефону; узаконить круг лиц, допускаемых к тем или иным фирменным секретам; запретить сотрудникам вести служебные переговоры с домашних телефонов.

Для передачи материалов, содержащих коммерческую тайну, используйте только закрытые каналы связи, которые организуются с помощью специальных средств защиты (скремблеры, шифраторы). Варианты использования средств шифрования для закрытия телефонных линий показаны на рис. 14.12, а упрощенная модель закрытого канала — на рис. 14.13. Если вы почувствовали, что за вами установлен контроль, используйте во время беседы систему условностей и сознательной дезинформации. Не называйте фамилии, отчества собеседника, если это позволяет этикет. Назначая время и место встречи, применяйте условности, которые логически вписываются в контекст разговора и понятны лишь собеседнику.

Приучите к определенному порядку ведения телефонных разговоров и членов вашей семьи: они не должны сообщать кому бы то ни было информацию о том, где вы находитесь и когда вернетесь домой.

Обнаружить подслушивающую аппаратуру на каналах связи так же сложно, как найти иголку в стоге сена, поэтому "иголку лучше не терять".

Любое электронное изделие при работе излучает так называемые побочные электромагнитные излучения и наводки. Очень распространены телефоны с кнопочным номеронабирателем типа ТА-Т, ТА-12 и т.д. При наборе номера и ведении переговоров благодаря техническим особенностям блока питания вся информация ретранслируется на десятках частот в СВ, КВ и УКВ диапазонах на расстояние до 200 м. В случае применении подобного телефона радиозакладки не нужны. Но это уже просто вопиющий случай. Обычно перехват осуществляется более сложно. С помощью малогабаритного индуктивного датчика можно улавливать побочные электромагнитные колебания автотрансформатора практически любого телефонного аппарата на расстоянии до полуметра. При этом также регистрируются набираемые номера и все разговоры.

Для защиты телефонных каналов связи необходимо, чтобы распределительная коробка телефонов фирмы находилась в помещении офиса и контролировалась службой безопасности или охраной.

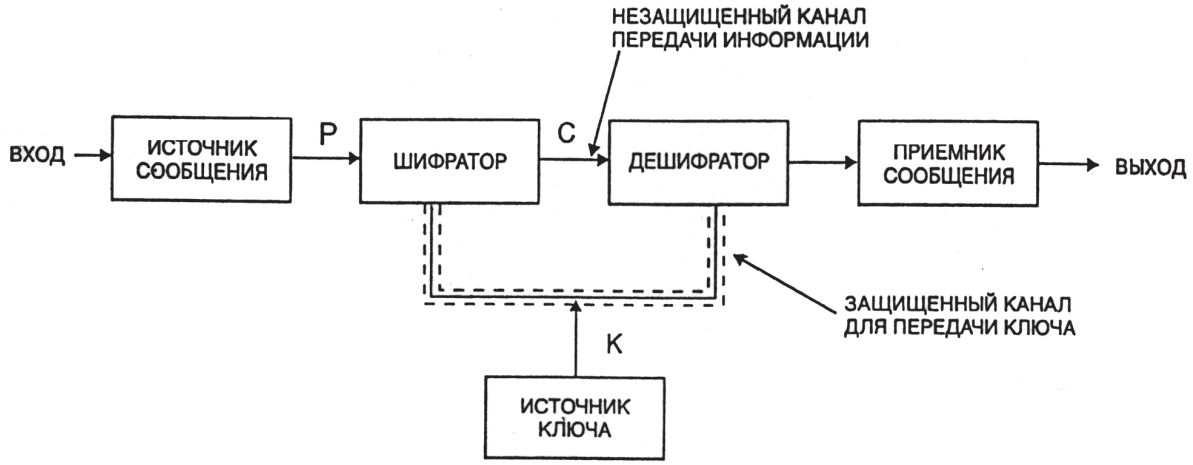


РИСУНОК 14.13. *Модель криптографической системы.*

Некоторые способы противодействия подслушиванию телефонных переговоров изложены в табл. 14.1.

Для ремонта телефонных аппаратов приглашайте проверенных специалистов. Заключите договор со специализированными предприятиями о проверке телефонных аппаратов и линий связи фирмы, а также распределительных коробок.

Если вы не знакомы с мастером узла связи, собирающимся ремонтировать телефоны в вашем офисе, не поленитесь, попросите у него служебное удостоверение, позвоните на узел связи и удостоверьтесь, что там действительно работает такой специалист, и именно он получал наряд на выполнение работ в вашей фирме. Если данные не подтвердились, срочно принимайте меры безопасности: постарайтесь сменить телефонный аппарат, вызовите знакомого монтера для проверки распределительной коробки, телефонных аппаратов. Усильте работу службы безопасности и охраны. Для передачи информации перейдите на запасные каналы связи, в том числе факс, телекс, телеграф (хотя и они могут контролироваться).

ОДНОСТОРОННИЕ МАСКИРАТОРЫ РЕЧИ

Надо знать

В настоящее время на рынке представлен только один такой прибор. Принцип его действия основан на том, что при приеме важного речевого сообщения от удаленного абонента владелец маскиратора включает режим защиты. При этом в телефонную линию подается интенсивный маскирующий шумовой сигнал в полосе частот, пропускаемых телефонным каналом, который распространяется по всей протяженности канала связи. Поскольку характеристика шумового сигнала известна, то в маскираторе происходит автоматическая компенсация помехи в поступившей на вход смеси полезного речевого и шумового сигналов с помощью адаптивного фильтра.

Маскиратор использует для компенсации шума адаптивный фильтр, имеющий некоторое время адаптации. Чем больше время адаптации, тем лучше компенсация помехи. Отсюда следует, что для уменьшения времени адаптации при маскировке следует использовать более однородный шумовой сигнал, характеристики которого легче вычислить злоумышленнику. Если для маскировки использовать шумовой сигнал, характеристики которого будут динамически изменяться, то, соответственно, снизится уровень компенсации помехи в трубке владельца маскиратора, но при этом задача злоумышленника серьезно осложнится.

(С.Е. Сталенков, Е.В. Шулика ЗАО НПЦ Фирма "НЕЛК")

В последнее время большой популярностью среди бизнесменов пользуются радиотелефоны и радиостанции различных типов. Как ни странно, но некоторые считают, что используя обычный телефон их могут подслушать, а в случае радиотелефона это практически невозможно. Однако следует помнить, что радиотелефон — это комплект из двух радиостанций, одна из которых является базовой, устанавливается стационарно и подключается к городской телефонной сети, вторая — подвижная. Следовательно, осуществлять прослушивание телефонных разговоров можно всеми, перечисленными выше способами. При этом нет необходимости устанавливать радиомикрофоны,телефонные закладки, использовать лазерные микрофоны или стетоскопы, достаточно приобрести качественный приемник, установить хорошую антенну и спокойно прослушивать разговоры.

Таблица 14.1. Способы противодействия подслушиванию телефонных переговоров.

СПОСОБЫ ПОДСЛУШИВАНЯ	СПОСОБЫ ПРОТИВОДЕЙСТВИЯ	
	ВЫЯВЛЕНИЕ	ЗАЩИТА
ЗА СЧЕТ МИКРОФОННОГО ЭФФЕКТА	Специальные измерения телефонных аппаратов на наличие микрофонного эффекта	1. Замена телефонного аппарата 2. Отключение от телефонной линии 3. Использование специальных устройств защиты
КОНТАКТНОЕ ПОДКЛЮЧЕНИЕ	Контроль телефонных линий: • на наличие подключений • на изменение напряжения питания	Прокладка кабелей в защищенных каналах
БЕЗКОНТАКТНОЕ ПОДКЛЮЧЕНИЕ	Контроль телефонных линий, определение опасных мест возможной установки индукционных датчиков	1. Использование экранированных кабелей 2. Исключение параллельного прокладывания линий
УСТАНОВКА ТЕЛЕФОННОЙ РАДИОЗАКЛАДКИ	Контроль наличия радиоизлучения в положении «поднятая трубка»	1. Постановка активных радиопомех 2. Изъятие радиозакладки
ВЫСОКОЧАСТОТНОЕ НАВЯЗЫВАНИЕ	Контроль наличия радиоизлучения	1. Постановка активных радиопомех 2. Установка в телефонную линию специальных фильтров высокой частоты

Способы и средства защиты телефонных переговоров (030)

Современные методы и технические средства защиты телефонных переговоров охватывают практически все возможные способы перехвата и сценарии их реализации. Выбор методов и технических средств защиты должен быть адекватным уровню потенциальных угроз, из этого принципа ведется и расчет необходимых затрат.

Специалисты выделяют две основные тактические разновидности защиты:

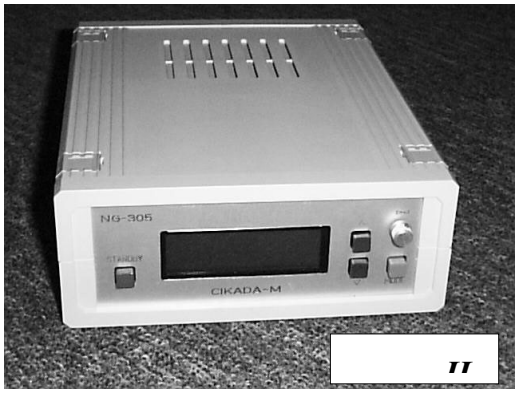
- средства физической защиты информации, включающие в себя постановщики заградительных помех, фильтры и нейтрализаторы;
- средства смысловой (криптографической) защиты.

Средства физической защиты информации (034)

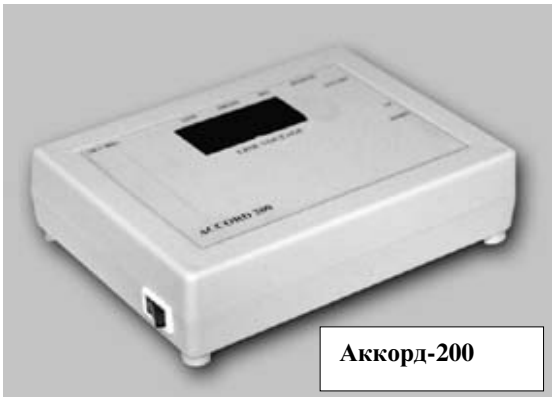
Для обеспечения фильтрации сигналов, возникающих в телефонной линии при положенной трубке за счет микрофонного эффекта или ВЧ-навязывания разработаны и выпускаются серийно недорогие приборы. В часности в Украине выпускаются приборы серии "Рикас" и "Базальт".

Нейтрализаторы предназначены для выведения из строя (прожигания) устройств, гальванически подключенных к телефонной линии. Это такие приборы, как "КС-1303", "Кобра". На выходе этих приборов создается кратковременное высоковольтное напряжение (до 1500 вольт), подаваемое в линию.

Устройств защиты телефонных переговоров, создающих заградительные помехи, великое множество, но



и



Аккорд-200

наиболее эффективными являются такие, как "Цикада-М", "Прокруст", "Аккорд-200", "Барьер-3", "Гром", обеспечивающих защиту от телефонного аппарата до АТС.

Принцип защиты, организованный этими устройствами состоит в том, что в линию выдается шумовая помеха вне полосы речевого сигнала и превышает его номинальный уровень на один-два порядка. Наличие интенсивной помехи выводит из линейного режима устройства, как гальванически подключенных к линии, так и индуктивных. Злоумышленник через свое устройство слышит сильный шум, забивающий речевой сигнал. Абоненты, ведущие переговоры слышат незначительный шум, не мешающий разговору, благодаря предварительной высокочастотной фильтрации выходного сигнала. Наиболее эффективно действует помеха, создаваемая устройствами "Цикада-М" и "Прокруст-2000. "Цикада-М" подает в линию (с использованием единой системы заземления аппаратуры АТС и нулевого провода бытовой сети 220 вольт) синфазный маскирующий сигнал акустического диапазона и парафазный сигнал в виде псевдослучайной последовательности ультразвукового диапазона, кроме того обеспечивается возможность создания участка телефонной линии с повышенной защитой, на котором гарантируется эффективное подавление всех технических средств негласного съема информации, в том числе индукционных датчиков, включенных в два провода с "обратной петлей". Для этого на конце участка линии с повышенной защитой (КРТ, распределительный шкаф) ставится фазокорректирующее устройство, входящее в комплект изделия.

Постановщики заградительной помехи достаточно эффективны, однако им присущи и некоторые недостатки.

Постановщики заградительной помехи обеспечивают защиту телефонной линии только на участке от самого прибора, к которому подключается штатный телефонный аппарат, до городской АТС. Поэтому остается опасность перехвата информации со стороны незащищенной линии противоположного абонента и на самой АТС. Поскольку частотный спектр помехи располагается выше частотного спектра речевого сигнала, то теоретически достаточно легко очистить полезный сигнал от помехи. И самое главное, эти приборы не защищают от съема информации непосредственно на АТС.

Несмотря на эти недостатки, благодаря относительно невысокой стоимости, постановщики заградительных помех получили наибольшее распространение среди других видов техники, предназначенной для защиты телефонных линий.

Кроме маскирующего шума, такие устройства, как "Аккорд-200", "Барьер-3" обеспечивают введение регулируемой вольтодобавки к напряжению, падающему на телефонном аппарате, путем электронной регулировки уровня постоянной составляющей в линии. В результате напряжение в линии при поднятой трубке будет не 10-15 вольт, а 25-35 вольт, что выводит из режима ЗУ, питающиеся от телефонной линии.

Устройства "Цикада-М", КТЛ-400, SP-18/T и некоторые другие при работе в сторожевом режиме сигнализируют о "пиратском" подключении к линии. Почти все из упоминаемых выше устройств защиты телефонных линий имеют режим активизации при положенной трубке защищаемого аппарата диктофонов, подключенных к линии через датчики любого типа с целью холостого проматывания ленты.

Отдельно из всего списка устройств защиты, используемых заградительную помеху, следует отметить маскираторы речи серии "Туман", использующие совершенно новую технологию защиты. Особенность в том, что шумовая помеха, действующая за пределами речевого диапазона частот, заменена на помеху в речевом диапазоне. Такая помеха формируется по псевдослучайному закону и меняется от сеанса к сеансу. Естественно такой детерминированный подход дает возмож-

ность скомпенсировать помеху на своем конце. Сеанс связи выглядит следующим образом.

Абонент №1, имеющий маскиратор, получает звонок от абонента №2, который хочет передать секретное сообщение, звонок может быть с любого телефона, включая телефон-автомат или междугородней связи. В момент передачи секретных сведений абонент №1 включает маскиратор, о чем предупреждает абонента №2. В линии возникает интенсивный шум, который слышит абонент №2, но продолжает свое сообщение, абонент №1 его прекрасно слышит и после окончания секретного сообщения выключает маскиратор, чтобы продолжить разговор по телефону в обычном режиме. Уровень маскирующего шума может быть выставлен настолько большим, что прослушать такую линию невозможно.

Недостатки односторонних маскираторов:

- ***Невозможность закрытия исходящих сообщений.*** Для преодоления этого ограничения потребуется установить маскираторы обоим абонентам, причем вести разговор в дуплексе им не удастся, поскольку каждому абоненту по очереди придется вручную включать режим маскировки и это вряд ли целесообразно т.к. проще, дешевле и надежнее воспользоваться скремблерами.

- ***Наличие сильного шума в трубке абонента,*** передающего сообщение. Услышав шум в трубке, неопытный абонент автоматически начнет передавать сообщение громким голосом, при этом соотношение амплитуд помехи и полезного сигнала на его плече телефонной линии снизится, что облегчит злоумышленнику задачу по очистке сообщения от помехи.

- ***Отсутствие в приборах такого класса противодействия перехвату речевой информации*** из помещения, по которому проходит телефонная линия, в режиме отбоя линии.

Средства криптографической защиты (034)

Криптографическая защита телефонных разговоров считается наиболее гарантированной защитой от перехвата по любым видам связи. ***Устройства криптографической защиты телефонных переговоров носят название скремблеров***. Наиболее распространенными являются скремблеры серии SCR (Россия) и "Орех" Украина. Для организации защиты необходимо иметь скремблеры у обоих абонентов и установить систему ввода ключей.

Скремблеры реализуют криптографическое преобразование как для аналоговых телефонных сообщений, так и для цифровых (вакодеры). Необходимо отметить, что речь при этом сохраняет приемлемую разборчивость, но опознать абонента по тембру голоса бывает затруднительно.

Работа таких систем делится на несколько этапов. На первом этапе речевое сообщение абонента обрабатывается по какому-либо алгоритму (кодируется) так, чтобы злоумышленник, перехвативший обработанный сигнал, не смог разобрать смысловое содержание исходного сообщения. Затем обработанный сигнал направляется в телефонную линию. На последнем этапе сигнал, полученный другим абонентом, преобразуется по обратному алгоритму (декодируется) в речевой сигнал с неизбежной потерей качества.

Для того, чтобы раскрыть смысловое содержание защищенного криптографическим способом телефонного разговора, злоумышленнику потребуется:

- наличие криптоаналитика;
- дорогостоящее оборудование;
- некоторое время для проведения криптоанализа.

Последний фактор может свести на нет все усилия, поскольку к моменту раскрытия сообщения высока вероятность того, что оно уже устарело. Кроме того, момент раскрытия может вообще не наступить.

Положительные стороны криптографической защиты телефонных переговоров.

Высокая степень защиты телефонных переговоров при использовании алгоритмов кодирования/декодирования высокой криптостойкости. Аналоговые алгоритмы (частотная инверсия) кодирования, которые довольно широко распространены в сравнительно не дорогих приборах, порядка 300−400 долларов за прибор, но они менее стойки. Более стойки алгоритмы с цифровой дискретизацией (вакодеры) с последующим шифрованием, но приборы использующие этот метод на много дороже.

К достоинствам криптографических систем следует отнести то, что защита происходит на всем протяжении линии связи и безразлично какой аппаратурой перехвата пользуется злоумышленник, он все равно не сможет в режиме реального времени расшифровать сообщение.

Недостатки криптографической защиты телефонных переговоров.

- Необходимость установки одинакового оборудования у всех абонентов, участвующих в закрытых переговорах.

- Потеря времени, необходимая для синхронизации аппаратуры и обмена ключами в начале сеанса защищенной связи.

- Временная задержка между моментом передачи сообщения и моментом приема.

- Потеря качества сигнала.
- Невозможность противостоять перехвату речевой информации в промежутках между телефонными переговорами. В настоящее время ни один из скремблеров не оборудован надежной системой предотвращения перехвата информации при положенной трубке.

Контроль информационных потоков состоит в их фильтрации, то есть в выборочном пропускании через экран, возможно, с выполнением некоторых преобразований и извещением отправителя о том, что его данным в пропуске отказано. Фильтрация осуществляется на основе набора правил, предварительно загруженных в экран и являющихся выражением сетевых аспектов политики безопасности организации.

Контроль телефонных разговоров является одним из самых распространенных видов промышленного шпионажа и действий преступных элементов. Это связано с незначительными затратами и риском, необязательностью захода в контролируемое помещение, разнообразием способов и мест съема информации.

В числе средств перехвата телефонных переговоров разнообразные устройства контактного и бесконтактного подключения к телефонным линиям, специальные телефонные "жучки" и т.д. Современные средства и методы защиты телефонных переговоров от перехвата противодействуют практически всему разнообразию средств их реализации.

Специалисты выделяют две основные технические разновидности противодействий:

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

Новые технические решения позволяют комплексно решать вопросы и обнаружения факта подслушивания телефонных переговоров и гарантированного подавления многих видов техники перехвата.

Резюме

Каналы связи — один из наиболее уязвимых компонентов ИС. В их составе можно указать большое число потенциально опасных мест, через которые злоумышленники могут проникнуть в ИС.

Особое место в подтверждении подлинности передачи сообщения занимает проблема защиты отправлений по каналам электронной почты, когда отправитель посылает сообщение получателю, который не является активным в момент пересылки сообщений. Поэтому процедура защиты электронной почты использует функцию, аналогичную функции подтверждения передачи, однако ее реализация требует специальных протоколов для надежного управления ключами, обеспечения целостности ресурсов и верификации отсроченных процедур.

Информация должна оставаться конфиденциальной как в процессе ее перемещения в пределах внутрифирменной сети, так и при передаче в другие сети. Никогда нельзя исключать возможность подслушивания данных, передаваемых по проводным каналам связи. А перехват “открытой информации”, передаваемой по линиям сотовой и радиорелейной связи, является для технически подготовленного противника еще более легкой задачей.

Шифрование сообщений позволяет преобразовать исходное сообщение (открытый текст) к нечитаемому виду; результат преобразования называют шифротекстом. Злоумышленник без знания секретного ключа шифрования не имеет возможности дешифровать шифротекст.

Для шифрования сообщений, как правило, используются симметричные криптосистемы. Несимметричные криптосистемы используются для формирования цифровой подписи и шифрования (формирования) симметричных ключей при их рассылке по каналам связи.

Среди протоколов распределения ключей на практике используется метод Диффи-Хеллмана и метод цифрового конверта. Среди методов цифровой подписи широкое применение нашли RSA-подобные алгоритмы и алгоритмы на основе метода Эль-Гамаля, стандартизованные в некоторых странах. Наиболее перспективным представляется использование усовершенствованного метода цифровой подписи Эль-Гамаля, который в последние годы стандартизован в США и России.

Защита от манипуляций над потоками сообщений может быть реализована путем включения дополнительной избыточной информации в виде номеров сообщений или отметок времени в шифрованном сообщении. Эта информация может быть естественной частью формата сообщения и по аналогии с основным содержанием должна быть защищена от возможных манипуляций.

Некоторые криптографические функции не обеспечивают удовлетворительной защиты без специальных секретов кодов подтверждения подлинности, которые должны представлять дополнительный механизм обработки исходного или шифрованного текста.

Выбрав правильную криптографическую систему, можно существенно упростить реализацию процедуры

подтверждения подлинности сообщений. Если шифрование применяется на физическом уровне, то в протоколе линии передачи данных достаточно использовать функции проверки с нормальным распределением ошибки. Если шифрование применяется на более высоком уровне, то аналогичные проверочные функции можно легко реализовать в формате сообщения (прикладной уровень протокола передачи данных).

Контроль телефонных разговоров является одним из самых распространенных видов промышленного шпионажа и действий преступных элементов. Это связано с незначительными затратами и риском, необязательностью захода в контролируемое помещение, разнообразием способов и мест съема информации.

В числе средств перехвата телефонных переговоров разнообразные устройства контактного и бесконтактного подключения к телефонным линиям, специальные телефонные "жучки" и т.д. Современные средства и методы защиты телефонных переговоров от перехвата противодействуют практически всему разнообразию средств их реализации.

Специалисты выделяют две основные технические разновидности противодействий:

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

Новые технические решения позволяют комплексно решать вопросы и обнаружения факта подслушивания телефонных переговоров и гарантированного подавления многих видов техники перехвата.