Лекция. Безопасность сетей

Защита информации – это комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и т.п. Поскольку утрата информации может происходить по сугубо техническим, объективным и неумышленным причинам, под это определение подпадают также и мероприятия, связанные с повышением надежности сервера из-за отказов или сбоев в работе винчестеров, недостатков в используемом программном обеспечении и т.д.

Следует заметить, что наряду с термином *"защита информации"* (применительно к компьютерным сетям) широко используется, как правило, в близком значении, термин "компьютерная безопасность".

Переход от работы на персональных компьютерах к работе в сети усложняет *защиту информации* по следующим причинам:

1. большое число пользователей в сети и их переменный состав. Защита на уровне имени и пароля пользователя недостаточна для предотвращения входа в сеть посторонних лиц;
2. значительная протяженность сети и наличие многих потенциальных каналов проникновения в сеть;
3. уже отмеченные недостатки в аппаратном и программном обеспечении, которые зачастую обнаруживаются не на предпродажном этапе, называемом бета- тестированием, а в процессе эксплуатации. В том числе неидеальны встроенные средства *защиты информации* даже в таких известных и "мощных" сетевых ОС, как Windows NT или NetWare.

В сети имеется много физических мест и каналов несанкционированного доступа к информации в сети. Каждое устройство в сети является потенциальным источником электромагнитного излучения из-за того, что соответствующие поля, особенно на высоких частотах, экранированы неидеально. Кроме электромагнитного излучения, потенциальную угрозу представляет бесконтактное электромагнитное воздействие на кабельную систему. Безусловно, в случае использования проводных соединений типа коаксиальных кабелей или витых пар возможно и непосредственное физическое подключение к кабельной системе. Если пароли для входа в сеть стали известны или подобраны, становится возможным несанкционированный вход в сеть с файл-сервера или с одной из рабочих станций. Наконец возможна утечка информации по каналам, находящимся вне сети:

- хранилище носителей информации,
- элементы строительных конструкций и окна помещений, которые образуют *каналы утечки конфиденциальной информации* за счет так

называемого микрофонного эффекта,
- телефонные, радио-, а также иные проводные и беспроводные каналы (в том числе каналы мобильной связи).

Любые дополнительные соединения с другими сегментами или подключение к Интернет порождают новые проблемы. Атаки на локальную сеть через подключение к Интернету для того, чтобы получить доступ к конфиденциальной информации, в последнее время получили широкое распространение, что связано с недостатками встроенной системы *защиты информации* в протоколах TCP/IP. Сетевые атаки через Интернет могут быть классифицированы следующим образом:

- Сниффер пакетов (sniffer – в данном случае в смысле фильтрация) – прикладная программа, которая использует сетевую карту, работающую в режиме promiscuous (не делающий различия) mode (в этом режиме все пакеты, полученные по физическим каналам, сетевой адаптер отправляет приложению для обработки).
- IP-спуфинг (spoof – обман, мистификация) – происходит, когда хакер, находящийся внутри корпорации или вне ее, выдает себя за санкционированного пользователя.
- Отказ в обслуживании (Denial of Service – DoS). Атака DoS делает сеть недоступной для обычного использования за счет превышения допустимых пределов функционирования сети, операционной системы или приложения.
- *DDoS* означает *distributed Denial of Service*: **распределённая атака типа «отказ в обслуживании»**. В этом случае речь идёт об огромной массе злонамеренных запросов, поступающих на атакуемый сервер из множества разных мест. Обычно такие атаки организуются посредством бот-сетей.
- Парольные атаки – их целью является завладение паролем и логином законного пользователя. Злоумышленники могут проводить парольные атаки, используя следующие методы: подмена IP-адреса (IP-спуфинг); прослушивание (сниффинг); простой перебор; использование метода «троянского коня». Парольные атаки часто проводятся с помощью методов социальной инженерии. **Данная тактика основана на анализе общедоступной информации о пользователе (место проживания, учёбы, дата рождения, кличка любимого питомца и многое другое)** и может нанести большой урон, т.к. обычно используются одни и те же учётные данные в разных сервисах. Получение общедоступной информации уменьшает трудозатраты злоумышленника.
- Атаки типа Man-in-the-Middle – вид атаки, когда злоумышленник тайно ретранслирует и при необходимости изменяет связь между двумя сторонами, которые считают, что они непосредственно общаются друг с другом. Вмешательство осуществляет в протокол передачи, перехватывая, удаляя или искажая информацию. Данная атака направлена **на обход взаимной аутентификации или отсутствие**

таковой и может увенчаться успехом только тогда, когда злоумышленник имеет возможность выдать себя за каждую конечную точку либо оставаться незамеченным в качестве промежуточного узла. Большинство криптографических протоколов включает в себя некоторую форму аутентификации конечной точки специально для предотвращения MITM-атак. Например, TLS может выполнять проверку подлинности одной или обеих сторон с помощью взаимно доверенного центра сертификации.

- **Атаки на уровне приложений.** В данном случае злоумышленники получают прямой доступ к приложениям корпоративной сети. Отдельный интерес для них представляют сервисы HTTP (TCP порт 80) и HTTPS (TCP порт 443), которые во многих сетях открыты именно на уровне приложений модели OSI (Open Systems Interconnection). В то же время устройства контроля доступа не могут эффективно идентифицировать злонамеренные действия, направленные на эти сервисы. К данной категории атак относят, например, запуск сценария на стороне клиента, инжекции кода SQL и т.д.
- **Сетевая разведка** – получение и обработка данных об информационной системе клиента, ресурсов информационной системы, используемых устройств и программного обеспечения и их уязвимостях, средств защиты, а также о границе проникновения в информационную систему. Сетевая разведка проводится в форме **запросов DNS**, **эхо-тестирования** (ping sweep) и **сканирования портов**. Запросы DNS помогают понять, кто владеет тем или иным доменом и какие адреса этому домену присвоены. Эхо-тестирование адресов, раскрытых с помощью DNS, позволяет увидеть, какие хосты реально работают в данной среде. Получив список хостов, хакер использует средства сканирования портов, чтобы составить полный список услуг, поддерживаемых этими хостами. И, наконец, хакер анализирует характеристики приложений, работающих на хостах. В результате добывается информация, которую можно использовать для взлома.
- **Вредоносное ПО типа «вирусы» или «черви».** Компьютерный вирус и компьютерный червь — это вредоносные программы, которые способны воспроизводить себя на компьютерах или через компьютерные сети. При этом пользователь не подозревает о заражении своего компьютера. Так как каждая последующая копия вируса или компьютерного червя также способна к самовоспроизведению, заражение распространяется очень быстро. Существует очень много различных типов компьютерных вирусов и компьютерных червей, большинство которых обладают высокой способностью к разрушению.

Классификация средств защиты информации

Защита информации в сети может быть улучшена за счет использования специальных генераторов шума, маскирующих побочные электромагнитные излучения и наводки, помехоподавляющих сетевых фильтров, устройств

зашумления сети питания, скремблеров (шифраторов телефонных переговоров), подавителей работы сотовых телефонов и т.д. Кардинальным решением является переход к соединениям на основе оптоволокна, свободным от влияния электромагнитных полей и позволяющим обнаружить факт несанкционированного подключения.

В целом средства обеспечения *защиты информации* в части предотвращения преднамеренных действий в зависимости от способа реализации можно разделить на группы:

1. Технические (аппаратные) средства. Это различные по типу устройства (механические, электромеханические, электронные и др.), которые аппаратными средствами решают задачи *защиты информации*. Они либо препятствуют физическому проникновению, либо, если проникновение все же состоялось, доступу к информации, в том числе с помощью ее маскировки. Первую часть задачи решают замки, решетки на окнах, защитная сигнализация и др. Вторую – упоминавшиеся выше генераторы шума, сетевые фильтры, сканирующие радиоприемники и множество других устройств, "перекрывающих" потенциальные *каналы утечки информации* или позволяющих их обнаружить. Преимущества технических средств связаны с их надежностью, независимостью от субъективных факторов, высокой устойчивостью к модификации. Слабые стороны – недостаточная гибкость, относительно большие объем и масса, высокая стоимость.
2. Программные средства включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др. Преимущества программных средств – универсальность, гибкость, надежность, простота установки, способность к модификации и развитию. Недостатки – ограниченная функциональность сети, использование части ресурсов файл-сервера и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров (их аппаратных средств).
3. Смешанные аппаратно-программные средства реализуют те же функции, что аппаратные и программные средства в отдельности, и имеют промежуточные свойства.
4. Организационные средства складываются из организационно-технических (подготовка помещений с компьютерами, прокладка кабельной системы с учетом требований ограничения доступа к ней и др.) и организационно-правовых (национальные законодательства и правила работы, устанавливаемые руководством конкретного предприятия). Преимущества организационных средств состоят в том, что они позволяют решать множество разнородных проблем, просты в реализации, быстро реагируют на нежелательные действия в сети, имеют неограниченные возможности модификации и развития. Недостатки – высокая зависимость от субъективных факторов, в том

числе от общей организации работы в конкретном подразделении.

По степени распространения и доступности выделяются программные средства, поэтому далее они рассматриваются более подробно

Шифрование данных представляет собой разновидность программных средств *защиты информации* и имеет особое значение на практике как единственная надежная *защита информации*, передаваемой по протяженным последовательным линиям, от утечки.

Шифрование - это обратимое преобразование информации в целях сокрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней.

Шифрование образует по сути последний, практически непреодолимый "рубеж" защиты от НСД. Понятие "шифрование" часто употребляется в связи с более общим понятием *криптографии*. *Криптография* включает способы и средства обеспечения конфиденциальности информации (в том числе с помощью шифрования) и аутентификации. **Конфиденциальность** – защищенность информации от ознакомления с ее содержанием со стороны лиц, не имеющих права доступа к ней. В свою очередь **аутентификация** представляет собой установление подлинности различных аспектов информационного взаимодействия: сеанса связи, сторон (идентификация), содержания (имитозащита) и источника (установление авторства с помощью цифровой подписи).

Число используемых программ шифрования ограничено, причем часть из них являются стандартами де-факто или де-юре. Однако даже если алгоритм шифрования не представляет собой секрета, произвести дешифрование (расшифрование) без знания закрытого ключа чрезвычайно сложно. Это свойство в современных программах шифрования обеспечивается в процессе многоступенчатого преобразования исходной открытой информации (plain text в англоязычной литературе) с использованием ключа (или двух ключей – по одному для шифрования и дешифрования). В конечном счете, любой сложный метод (алгоритм) шифрования представляет собой комбинацию относительно простых методов.

Классические алгоритмы шифрования данных

Имеются следующие "классические" методы шифрования:

- подстановка (простая – одноалфавитная, многоалфавитная однопетлевая, многоалфавитная многопетлевая);
- перестановка (простая, усложненная);
- гаммирование (смешивание с короткой, длинной или неограниченной маской).

Устойчивость каждого из перечисленных методов к дешифрованию без знания ключа характеризуется количественно с помощью показателя Sк

представляющего собой минимальный объем зашифрованного текста который может быть дешифрован посредством статистического анализа.

Подстановка предполагает использование альтернативного алфавита (или нескольких) вместо исходного. В случае простой подстановки для символов английского алфавита можно предложить, например, следующую замену (см табл. 1).

Таблица 1. Пример замены символов при подстановке

Исходный алфавит	A	B	C	D	E	F	G	H	I	J	K	L	...	X	Y	Z
Альтернативный алфавит	S	O	U	H	K	T	L	X	N	W	M	Y	...	A	P	J

Тогда слово "cache" в зашифрованном виде представляется как "usuxk".

Существует, однако, возможность дешифрования сообщения с помощью известной статистической частоты повторяемости символов в произвольном достаточно длинном тексте. Символ E встречается чаще всего – в среднем 12 раза на каждые 1000 символов или в 12,3% случаев, далее следуют символы T – 9,6%, A – 8,1%, O – 7,9%, N – 7,2%, I – 7,2%, S – 6,6%, R – 6,0%, H – 5,1%, L - 4,0% и т.д. Приведенные цифры могут, конечно, несколько варьироваться в зависимости от источника информации, из которого они были взяты, что не изменяет принципиально ситуации. Показатель устойчивости к дешифрованию Sк не превышает 20...30. При многоалфавитной подстановке можно добиться того, что в зашифрованном тексте все символы будут встречаться примерно с одинаковой частотой, что существенно затруднит дешифрование без знания альтернативных алфавитов и порядка, в котором они использовались при шифровании.

В многоалфавитных подстановках для замены символов исходного текста используется не один, а несколько алфавитов. Обычно алфавиты для замены образованы из символов исходного алфавита, записанных в другом порядке. Примером многоалфавитной подстановки может служить схема, основанная на использовании таблицы Вижинера.
В этом методе для шифрования используется таблица, представляющая собой квадратную матрицу с числом элементов NxN, где N — количество символов в алфавите (таблица 2). В первой строке матрицы записывают буквы в порядке очередности их в исходном алфавите, во второй — ту же последовательность букв, но с циклическим сдвигом влево на одну позицию, в третьей — со сдвигом на две позиции и т. д.

Таблица 2. Подготовка таблицы для многоалфавитного шифрования

АБВГДЕ.....	.....ЭЮЯ
БВГДЕЖ.....	.....ЮЯА
ВГДЕЖЗ.....	.....ЯАБ
ГДЕЖЗИ.....	.....АБВ
ДЕЖЭИК.....	.....БВГ
ЕЖЗИКЛ.....	.....ВГД
.....	.....
ЯАБВГД.....	.....ЬЭЮ

Для шифрования текста выбирают ключ, представляющий собой некоторое слово или набор символов исходного алфавита. Далее из полной матрицы выписывают подматрицу шифрования, включающую первую строку и строки матрицы, начальными буквами которых являются последовательно буквы ключа (например, если выбрать ключ "весна", то таблица шифрования будет такой, как на таблица 3).

Таблица 3. Составление подматрицы шифрования

АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ
ВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБ
ЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГД
НОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЖЗИКЛМ
СТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЖЗИКЛМНОПР

В процессе шифрования под каждой буквой шифруемого текста записывают буквы ключа, повторяющие ключ требуемое число раз, затем шифруемый текст по таблице шифрования (таблица 3) заменяют буквами, расположенными на пересечениях линий, соединяющих буквы текста первой строки таблицы и буквы ключа, находящейся под ней (рис. 1).

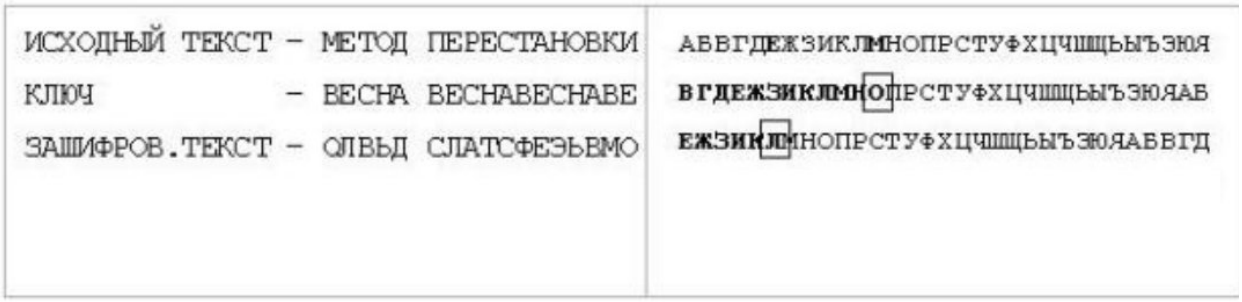

Рис. 1. Механизм многоалфавитной подстановки

Например, под первой буквой исходного текста "М" записана

буква "В" ключа. В таблице кодирования находим столбец, начинающийся с "М" и строку, начинающуюся с "В". На их пересечении располагается буква "О". Она и будет первым символом зашифрованного сообщения (на рис. 2.5 эта буква выделена прямоугольной рамочкой). Следующая буква исходного сообщения – "Е", символ ключа – тоже "Е". Находим пересечение строки, начинающейся с "Е", и столбца, начинающегося с "Е". Это будет буква "Л" – второй символ зашифрованного сообщения.

Перестановка потенциально обеспечивает большую по сравнению с подстановкой устойчивость к дешифрованию и выполняется с использованием цифрового ключа или эквивалентного ключевого слова, как это показано на следующем примере (см. табл. 4). Цифровой ключ состоит из неповторяющихся цифр, а соответствующее ему ключевое слово – из неповторяющихся символов. Исходный текст (plain text) записывается под ключом построчно. Зашифрованное сообщение (cipher text) выписывается по столбцам в том порядке, как это предписывают цифры ключа или в том порядке, в котором расположены отдельные символы ключевого слова.

Таблица 4. Пример использования простой перестановки

Ключевое слово	S	E	C	U	R	I	T	Y
Цифровой ключ	5	2	1	7	4	3	6	8
Исходный текст (plain text), записанный построчно	T	R	A	N	S	P	O	S
	I	T	I	O	N	α	I	S
	α	T	H	E	α	E	N	C
	I	P	H	E	R	α	M	E
	T	H	O	D	α	α	α	α

α – служебный символ, в данном случае означает пробел

Для рассматриваемого примера зашифрованное сообщение будет выглядеть следующим образом:

AIHHORTTPHPαEααα…SSCEα.

Гаммирование (смешивание с маской) основано на побитном сложении по модулю 2 (в соответствии с логикой ИСКЛЮЧАЮЩЕЕ ИЛИ) исходного сообщения с заранее выбранной двоичной последовательностью (маской). Компактным представлением маски могут служить числа в десятичной системе счисления или некоторый текст (в данном случае рассматриваются внутренние коды символов – для английского текста таблица ASCII). На рис. 3 показано, как исходный символ "A" при сложении с маской 0110 1001 переходит в символ "(" в зашифрованном сообщении.

$$\begin{array}{ll} \text{"A"} & \rightarrow 41_{16} = 0100\ 0001_2 \\ \oplus\ \text{маска} & \rightarrow 69_{16} = 0110\ 1001_2 \\ \hline \text{"("} & \rightarrow 28_{16} = 0010\ 1000_2 \end{array}$$

Рис. 3. Пример использования гаммирования

Операция суммирования по модулю 2 (ИСКЛЮЧАЮЩЕЕ ИЛИ) является обратимой, так что при сложении с той же маской (ключом) зашифрованного сообщения получается исходный текст (происходит дешифрование). В качестве маски (ключа) могут использоваться константы типа p или e и тогда маска будет иметь конечную длину. Наибольшую устойчивость к дешифрованию может обеспечить применение маски с бесконечной длиной, которая образована генератором случайных (точнее, псевдослучайных) последовательностей. Такой генератор легко реализуется аппаратными или программными средствами, например, с помощью сдвигового регистра с обратными связями, который используется при вычислении помехоустойчивого циклического кода. Точное воспроизведение псевдослучайной последовательности в генераторе на приемном конце линии обеспечивается при установке такого же исходного состояния (содержимого сдвигового регистра) и той же структуры обратных связей, что и в генераторе на передающем конце.

Перечисленные "классические" методы шифрования (подстановка, перестановка и гаммирование) являются линейными в том смысле, что длина зашифрованного сообщения равна длине исходного текста. Возможно **нелинейное преобразование** типа подстановки вместо исходных символов (или целых слов, фраз, предложений) заранее выбранных комбинаций символов другой длины. Эффективна также *защита информации* методом рассечения-разнесения, когда исходные данные разбиваются на блоки, каждый из которых не несет полезной информации, и эти блоки хранятся и передаются независимо друг от друга. Для текстовой информации отбор данных для таких блоков может производиться по группам, которые включают фиксированное число бит, меньшее, чем число бит на символ в таблице кодировки. В последнее время становится популярной так называемая компьютерная стеганография (от греческих слов steganos - секрет, тайна и graphy – запись), представляющая собой сокрытие сообщения или файла в другом сообщении или файле. Например, можно спрятать зашифрованный аудио- или видеофайл в большом информационном или графическом файле. Объем файла – контейнера должен быть больше объема исходного файла не менее чем в восемь раз. Примерами распространенных программ, реализующих компьютерную стеганографию, являются S – Tools (для ОС Windows’95/NT). и Steganos for Windows’95. Собственно шифрование информации осуществляется с применением стандартных или нестандартных алгоритмов.

Стандартные методы шифрования (национальные или международные) для повышения степени устойчивости к дешифрованию реализуют несколько этапов (шагов) шифрования, на каждом из которых используются различные "классические" методы шифрования в соответствии с выбранным ключом (или ключами). Существуют две принципиально различные группы стандартных методов шифрования:

- шифрование с применением одних и тех же ключей (шифров) при шифровании и дешифровании (*симметричное шифрование* или системы с закрытыми ключами – private-key systems);
- шифрование с использованием открытых ключей для шифрования и закрытых – для дешифрования (*несимметричное шифрование* или системы с открытыми ключами – public-key systems).

Строгое математическое описание алгоритмов стандартных методов шифрования слишком сложно. Для пользователей важны в первую очередь "потребительские" свойства различных методов (степень устойчивости к дешифрованию, скорость шифрования и дешифрования, порядок и удобство распространения ключей), которые и рассматриваются ниже.

Для дальнейшего повышения устойчивости к дешифрованию могут применяться последовательно несколько стандартных методов или один метод шифрования (но с разными ключами).

Стандартные методы шифрования и криптографические системы

Стандарт шифрования США DES (Data Encryption Standard – стандарт шифрования данных) относится к группе методов *симметричного шифрования* и действует с 1976 г. Число шагов – 16. Длина ключа – 56 бит, из которых 8 бит – проверочные разряды четности/нечетности. Долгое время степень устойчивости к дешифрованию этого метода считалась достаточной, однако в настоящее время он устарел. Вместо DES предлагается "тройной DES" – **3DES**, в котором алгоритм DES используется 3 раза, обычно в последовательности "шифрование – дешифрование – шифрование" с тремя разными ключами на каждом этапе.

Надежным считается алгоритм **IDEA** (International Data Encryption Algorithm), разработанный в Швейцарии и имеющий длину ключа 128 бит.

Отечественный **ГОСТ28147-89** – это аналог DES, но с длиной ключа 256 бит, так что его степень устойчивости к дешифрованию изначально существенно выше. Важно также и то, что в данном случае предусматривается целая система защиты, которая преодолевает "родовой" недостаток *симметричных методов шифрования* – возможность подмены сообщений. Такие усовершенствования, как имитовставки, хэш-функции и электронные цифровые подписи позволяют "авторизовать" передаваемые сообщения.

К достоинствам *симметричных методов шифрования* относится высокая скорость шифрования и дешифрования, к недостаткам – малая степень защиты в случае, если ключ стал доступен третьему лицу.

Довольно популярны, особенно при использовании электронной почты в Интернет, *несимметричные методы шифрования* или системы с открытыми

ключами – public-key systems. К этой группе методов относится, в частности, **PGP** (Pretty Good Privacy – достаточно хорошая секретность). Каждый пользователь имеет пару ключей. Открытые ключи предназначены для шифрования и свободно рассылаются по сети, но не позволяют произвести дешифрование. Для этого нужны секретные (закрытые) ключи. Принцип шифрования в данном случае основывается на использовании так называемых односторонних функций. Прямая функция $x \rightarrow f(x)$ легко вычисляется на основании открытого алгоритма (ключа). Обратное преобразование. $f(x) \rightarrow x$ без знания закрытого ключа затруднено и должно занимать довольно длительное время, которое и определяет степень "трудновычислимости" односторонней функции.

Идея системы с открытыми ключами может быть пояснена следующим образом (табл. 9.3). Для шифрования сообщений можно взять обычную телефонную книгу, в которой имена абонентов расположены в алфавитном порядке и предшествуют телефонным номерам. У пользователя имеется возможность выбора соответствия между символом в исходном тексте и именем абонента, то есть это многоалфавитная система. Ее степень устойчивости к дешифрованию выше. Легальный пользователь имеет "обратный" телефонный справочник, в котором в первом столбце располагаются телефонные номера по возрастанию, и легко производит дешифрование. Если же такового нет, то пользователю предстоит утомительное и многократное просматривание доступного прямого справочника в поисках нужных телефонных номеров. Это и есть практическая реализация трудно-вычислимой функции. Сам по себе метод шифрования на основе телефонных справочников вряд ли перспективен хотя бы из-за того, что никто не мешает потенциальному взломщику составить "обратный" телефонный справочник. Однако в используемых на практике методах шифрования данной группы в смысле надежности защиты все обстоит благополучно.

Таблица 9.3. Пример шифрования в системе с открытыми ключами

Исходное слово	Выбранное имя абонента	Зашифрованное сообщение (те
S	Scott	3541920
A	Adleman	4002132
U	Ullman	7384502
N	Nivat	5768115
A	Aho	7721443

Другая известная система с открытыми ключами – **RSA**.

Несимметричные методы шифрования имеют преимущества и недостатки, обратные тем, которыми обладают *симметричные методы*. В частности, в *несимметричных методах* с помощью посылки и анализа специальных служебных сообщений может быть реализована процедура аутентификации (проверки легальности источника информации) и целостности (отсутствия подмены) данных. При этом выполняются операции шифрования и

дешифрования с участием открытых ключей и секретного ключа данного пользователя. Таким образом, симметричные системы можно с достаточным основанием отнести к полноценным криптографическим системам. В отличие от *симметричных методов шифрования*, проблема рассылки ключей в *несимметричных методах* решается проще – пары ключей (открытый и закрытый) генерируются "на месте" с помощью специальных программ. Для рассылки открытых ключей используются такие технологии как **LDAP** (Lightweight Directory Access Protocol – протокол облегченного доступа к справочнику). Рассылаемые ключи могут быть предварительно зашифрованы с помощью одного из *симметричных методов шифрования*.

Традиционные и обязательные для современных криптографических систем способы обеспечения аутентификации и проверки целостности получаемых данных (хэш-функции и цифровые подписи), которые реализуются непосредственными участниками обмена, не являются единственно возможными. Распространен также способ, осуществляемый с участием сторонней организации, которой доверяют все участники обменов. Речь идет об использовании так называемых цифровых сертификатов – посылаемых по сети сообщений с цифровой подписью, удостоверяющей подлинность открытых ключей.

Программные средства защиты информации

Встроенные средства защиты информации в сетевых ОС доступны, но не всегда, как уже отмечалось, могут полностью решить возникающие на практике проблемы. Например, сетевые ОС NetWare 3.x, 4.x позволяют осуществить надежную "эшелонированную" защиту данных от аппаратных сбоев и повреждений. Система SFT (System Fault Tolerance – система устойчивости к отказам) компании Novell включает три основные уровня:

- SFT Level I предусматривает, в частности, создание дополнительных копий FAT и Directory Entries Tables, немедленную верификацию каждого вновь записанного на файловый сервер блока данных, а также резервирование на каждом жестком диске около 2% от объема диска. При обнаружении сбоя данные перенаправляются в зарезервированную область диска, а сбойный блок помечается как "плохой" и в дальнейшем не используется.
- SFT Level II содержит дополнительные возможности создания "зеркальных" дисков, а также дублирования дисковых контроллеров, источников питания и интерфейсных кабелей.
- SFT Level III позволяет применять в локальной сети дублированные серверы, один из которых является "главным", а второй, содержащий копию всей информации, вступает в работу в случае выхода "главного" сервера из строя.

Система контроля и ограничения прав доступа в сетях NetWare (защита от несанкционированного доступа) также содержит несколько уровней:

- уровень начального доступа (включает имя и пароль пользователя,

систему учетных ограничений – таких как явное разрешение или запрещение работы, допустимое время работы в сети, место на жестком диске, занимаемое личными файлами данного пользователя, и т.д.);
- уровень прав пользователей (ограничения на выполнение отдельных операций и/или на работу данного пользователя, как члена подразделения, в определенных частях файловой системы сети);
- уровень атрибутов каталогов и файлов (ограничения на выполнение отдельных операций, в том числе удаления, редактирования или создания, идущие со стороны файловой системы и касающиеся всех пользователей, пытающихся работать с данными каталогами или файлами);
- уровень консоли файл-сервера (блокирование клавиатуры файл-сервера на время отсутствия сетевого администратора до ввода им специального пароля).

Однако полагаться на эту часть системы *защиты информации* в ОС NetWare можно не всегда. Свидетельством тому являются многочисленные инструкции в Интернете и готовые доступные программы, позволяющие взломать те или иные элементы защиты от несанкционированного доступа.

То же замечание справедливо по отношению к более поздним версиям ОС NetWare (вплоть до последней 6-й версии) и к другим "мощным" сетевым ОС со встроенными средствами *защиты информации* (Windows NT, UNIX). Дело в том, что *защита информации* – это только часть тех многочисленных задач, которые решаются сетевыми ОС. Усовершенствование одной из функций в ущерб другим (при понятных разумных ограничениях на объем, занимаемый данной ОС на жестком диске) не может быть магистральным направлением развития таких программных продуктов общего назначения, которыми являются сетевые ОС. В то же время в связи с остротой проблемы *защиты информации* наблюдается тенденция интеграции (встраивания) отдельных, хорошо зарекомендовавших себя и ставших стандартными средств в сетевые ОС, или разработка собственных "фирменных" аналогов известным программам *защиты информации*. Так, в сетевой ОС NetWare 4.1 предусмотрена возможность кодирования данных по принципу "открытого ключа" (алгоритм RSA) с формированием электронной подписи для передаваемых по сети пакетов.

Специализированные программные средства защиты информации от несанкционированного доступа обладают в целом лучшими возможностями и характеристиками, чем встроенные средства сетевых ОС. Кроме программ шифрования и криптографических систем, существует много других доступных внешних средств *защиты информации*. Из наиболее часто упоминаемых решений следует отметить следующие две системы, позволяющие ограничить и контролировать информационные потоки.

1. Firewalls – брандмауэры (дословно firewall – огненная стена). Между локальной и глобальной сетями создаются специальные

промежуточные серверы, которые инспектируют и фильтруют весь проходящий через них трафик сетевого/транспортного уровней. Это позволяет резко снизить угрозу несанкционированного доступа извне в корпоративные сети, но не устраняет эту опасность полностью. Более защищенная разновидность метода – это способ маскарада (masquerading), когда весь исходящий из локальной сети трафик посылается от имени firewall-сервера, делая локальную сеть практически невидимой.

2. Proxy-servers (proxy – доверенность, доверенное лицо). Весь трафик сетевого/транспортного уровней между локальной и глобальной сетями запрещается полностью – маршрутизация как таковая отсутствует, а обращения из локальной сети в глобальную происходят через специальные серверы-посредники. Очевидно, что при этом обращения из глобальной сети в локальную становятся невозможными в принципе. Этот метод не дает достаточной защиты против атак на более высоких уровнях – например, на уровне приложения (вирусы, код Java и JavaScript).