Билет № 23. 1
ЗАЩИТА ИНОРМАЦИИ В ЛОКАЛЬНЫХ СЕТЯХ.

Кузнецов Николай

5 курс 3 группа

ФТиП МПГУ

Москва 2012

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

Классификация угроз

Задачу защиты информации в локальной сети усложняет:

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. система заземления вместе с кабельной системой и сетью электропитания может служить каналом доступа к информации в сети, в том числе на участках, находящихся вне зоны контролируемого доступа и потому особенно уязвимых.
4. атаки на локальную сеть через подключение к Интернету (в последнее время получили широкое распространение)
5. телефонные, радио-, а также иные проводные и беспроводные каналы (в том числе каналы мобильной связи).

Классификация средств защиты информации

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.
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.
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).

Криптография. Понятия и определения.

- **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.
- **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
- **Аутентификация** представляет собой установление подлинности различных аспектов информационного взаимодействия: сеанса связи, сторон (идентификация), содержания (имитозащита) и источника (установление авторства с помощью цифровой подписи).

Классические алгоритмы шифрования данных

В криптографии 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.

- Метод подстановки.

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".

- Метод перестановки

Выполняется с использованием цифрового ключа или эквивалентного ключевого слова. Цифровой ключ состоит из неповторяющихся цифр, а соответствующее ему ключевое слово – из неповторяющихся символов.

Пример замены символов при перестановки:

Ключевое слово	S	E	C	U	R	I	T	Y
Цифровой код	5	2	1	7	4	3	6	8

- Метод гаммирования

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 качестве маски (ключа) могут использоваться константы типа Π или e.

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.

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).

Стандартные криптографические системы

- Симметричное шифрование

  В США DES (Data Encryption Standard – стандарт шифрования данных) действует с 1976 г. Число шагов – 16. Длина ключа – 64 бита, из которых 8 бит – проверочные разряды четности/нечетности. В настоящее время он устарел и 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, его степень устойчивости к дешифрованию изначально существенно выше.

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.

- Несимметричные методы шифрования

Или системы с открытыми ключами – public-key systems.

Алгоритм **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 >> f(x) легко вычисляется на основании открытого алгоритма (ключа). Обратное преобразование. f(x) >> x без знания закрытого ключа затруднено и должно занимать довольно длительное время, которое и определяет степень "трудновычислимости" односторонней функции.

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

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.

Программные средства защиты

Встроенные средства защиты информации в сетевых ОС доступны, но не всегда 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.
- Система контроля и ограничения прав доступа в сетях NetWare (защита от несанкционированного доступа) также содержит несколько уровней.

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.

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 две системы, позволяющие ограничить и контролировать информационные потоки.

- Firewalls – брандмауэры (дословно firewall – огненная стена).
- Proxy-servers (proxy – доверенность, доверенное лицо).