Лекция № 21

ЗАЩИТА ИНФОРМАЦИИ, АНТИВИРУСНАЯ ЗАЩИТА

Информация является одним из наиболее ценных ресурсов любой компании, поэтому обеспечение защиты информации является одной из важнейших и приоритетных задач.

Безопасность информационной системы - это свойство, заключающее в способности системы обеспечить ее нормальное функционирование, то есть обеспечить целостность и секретность информации.

Для обеспечения целостности и конфиденциальности информации необходимо обеспечить защиту информации от случайного уничтожения или несанкционированного доступа к ней.

Под *целостностью* понимается невозможность несанкционированного или случайного уничтожения, а также модификации информации.

Под *конфиденциальностью* информации - невозможность утечки и несанкционированного завладения хранящейся, передаваемой или принимаемой информации.

Известны следующие источники угроз безопасности информационных систем:

- антропогенные источники, вызванные случайными или преднамеренными действиями субъектов;
- техногенные источники, приводящие к отказам и сбоям технических и программных средств из-за устаревших программных и аппаратных средств или ошибок в ПО;
- стихийные источники, вызванные природными катаклизмами или форс-мажорными обстоятельствами.

В свою очередь антропогенные источники угроз делятся на:

- внутренние (воздействия со стороны сотрудников компании) и внешние (несанкционированное вмешательство посторонних лиц из внешних сетей общего назначения) источники;
- непреднамеренные (случайные) и преднамеренные действия субъектов.

Существует достаточно много возможных направлений утечки информации и путей несанкционированного доступа к ней в системах и сетях:

- перехват информации;
- модификация информации (исходное сообщение или документ изменяется или подменяется другим и отсылается адресату);
- подмена авторства информации (кто-то может послать письмо или документ от вашего имени);

- использование недостатков операционных систем и прикладных программных средств;
- копирование носителей информации и файлов с преодолением мер защиты;
- незаконное подключение к аппаратуре и линиям связи;
- маскировка под зарегистрированного пользователя и присвоение его полномочий;
- введение новых пользователей;
- внедрение компьютерных вирусов и так далее.

Для обеспечения безопасности информационных систем применяют системы защиты информации, которые представляют собой комплекс организационно- технологических мер, программно- технических средств и правовых норм, направленных на противодействие источникам угроз безопасности информации.

При комплексном подходе методы противодействия угрозам интегрируются, создавая архитектуру безопасности систем.

Необходимо отметить, что любая системы защиты информации не является полностью безопасной.

Всегда приходиться выбирать между уровнем защиты и эффективностью работы информационных систем.

К средствам защиты информации ИС от действий субъектов относятся:

- средства защита информации от несанкционированного доступа;
- защита информации в компьютерных сетях;
- криптографическая защита информации;
- электронная цифровая подпись;
- защита информации от компьютерных вирусов.

Средства защиты информации от несанкционированного доступа

Получение доступа к ресурсам информационной системы предусматривает выполнение трех процедур:

- идентификация,
- аутентификация,
- авторизация.

*Идентификация** - присвоение пользователю (объекту или субъекту ресурсов) уникальных имен и кодов (идентификаторов).

*Аутентификация** - установление подлинности пользователя, представившего идентификатор или проверка того, что лицо или устройство, сообщившее идентификатор является действительно тем, за кого оно себя выдает.

Наиболее распространенным способом аутентификации является присвоение пользователю пароля и хранение его в компьютере.

*Авторизация** - проверка полномочий или проверка права пользователя на доступ к конкретным ресурсам и выполнение определенных операций над ними.

Авторизация проводится с целью разграничения прав доступа к сетевым и компьютерным ресурсам.

Защита информации в компьютерных сетях

Локальные сети предприятий очень часто подключаются к сети Интернет.

Для защиты локальных сетей компаний, как правило, применяются межсетевые экраны - брандмауэры (firewalls).

Экран (firewall) - это средство разграничения доступа, которое позволяет разделить сеть на две части (граница проходит между локальной сетью и сетью Интернет) и сформировать набор правил, определяющих условия прохождения пакетов из одной части в другую.

Экраны могут быть реализованы как аппаратными средствами, так и программными.

Криптографическая защита информации

Для обеспечения секретности информации применяется ее шифрование или криптография. Криптология разделяется на два направления — криптографию и криптоанализ.

Цели этих направлений прямо противоположны.

Криптография занимается поиском и исследованием методов шифрования информации.

Она даёт возможность преобразовывать информацию таким образом, что её прочтение (восстановление) возможно только при знании ключа.

Сфера интересов *криптоанализа* — исследование возможностей расшифровки информации без знания ключей.

Для шифрования используется алгоритм или устройство, которое реализует определенный алгоритм.

Управление шифрованием осуществляется с помощью изменяющегося кода ключа.

*Ключ** - информация, необходимая для беспрепятственного шифрования и дешифрования текста.

Извлечь зашифрованную информацию можно только с помощью ключа.

Криптография - это очень эффективный метод, который повышает безопасность передачи данных в компьютерных сетях и при обмене информацией между удаленными компьютерами.

Электронная цифровая подпись

Для исключения возможности модификации исходного сообщения или подмены этого сообщения другим необходимо передавать сообщение вместе с электронной подписью.

Электронная цифровая подпись - это последовательность символов, полученная в результате криптографического преобразования исходного сообщения с использованием закрытого ключа и позволяющая определять целостность сообщения и принадлежность его автору при помощи открытого ключа.

Сообщение, зашифрованное с помощью закрытого ключа, называется электронной цифровой подписью.

Отправитель передает незашифрованное сообщение в исходном виде вместе с цифровой подписью.

Получатель с помощью открытого ключа расшифровывает набор символов сообщения из цифровой подписи и сравнивает их с набором символов незашифрованного сообщения.

При полном совпадении символов можно утверждать, что полученное сообщение не модифицировано и принадлежит его автору.

Защита информации от компьютерных вирусов

*Компьютерный вирус** – это небольшая вредоносная программа, которая самостоятельно может создавать свои копии и внедрять их в программы (исполняемые файлы), документы, загрузочные сектора носителей данных и распространяться по каналам связи.

Одним из способов классификации компьютерных вирусов – это разделение их по следующим основным признакам:

- среда обитания;
- особенности алгоритма;
- способы заражения;
- степень воздействия (безвредные, опасные, очень опасные).

В зависимости от среды обитания основными типами компьютерных вирусов являются:

- Программные (поражают файлы с расширением .COM и .EXE) вирусы;
- Загрузочные вирусы;
- Макровирусы;
- Сетевые вирусы.

Программные вирусы – это вредоносный программный код, который внедрен внутрь исполняемых файлов (программ).

Вирусный код может воспроизводить себя в теле других программ – этот процесс называется размножением.

По прошествии определенного времени, создав достаточное количество копий, программный вирус может перейти к разрушительным действиям – нарушению работы программ и операционной системы, удаляя информации, хранящиеся на жестком диске. Этот процесс называется вирусной атакой.

Загрузочные вирусы – поражают не программные файлы, а загрузочный сектор магнитных носителей (гибких и жестких дисков).

Сетевые вирусы пересылаются с компьютера на компьютер, используя для своего распространения компьютерные сети, электронную почту и другие каналы.

Макровирусы – поражают документы, которые созданы в прикладных программах, имеющих средства для исполнения макрокоманд.

К таким документам относятся документы текстового процессора WORD, табличного процессора Excel.

Заражение происходит при открытии файла документа в окне программы, если в ней не отключена возможность исполнения макрокоманд.

По алгоритмам работы различают компьютерные вирусы:

- Черви (пересылаются с компьютера на компьютер через компьютерные сети, электронную почту и другие каналы);
- Вирусы-невидимки (Стелс-вирусы);
- Троянские программы;
- Программы – мутанты;
- Логические бомбы и др.

Основные признаки появления вируса в ПК:

- медленная работа компьютера;
- зависания и сбои в работе компьютера;
- изменение размеров файлов;
- уменьшение размера свободной оперативной памяти;
- значительное увеличение количества файлов на диске;
- исчезновение файлов и каталогов или искажение их содержимого;
- изменение даты и времени модификации файлов и др.

- Чтобы предотвратить заражение вирусами и атаки троянских коней, необходимо выполнять некоторые рекомендации:
- Не запускайте программы, полученные из Интернета или в виде вложения в сообщение электронной почты без проверки на наличие в них вируса;
- Необходимо проверять все внешние диски на наличие вирусов, прежде чем копировать или открывать содержащиеся на них файлы или выполнять загрузку компьютера с таких дисков;
- Необходимо установить антивирусную программу и регулярно пользоваться ею для проверки компьютеров. Оперативно пополняйте базу данных антивирусной программы набором файлов сигнатур вирусов, как только появляются новые сигнатуры;

- Необходимо регулярно сканировать жесткие диски в поисках вирусов. Сканирование обычно выполняется автоматически при каждом включении ПК и при размещении внешнего диска в считывающем устройстве. При сканировании антивирусная программа ищет вирус путем сравнения кода программ с кодами известных ей вирусов, хранящихся в базе данных;
- Создавать надежные пароли, чтобы вирусы не могли легко подобрать пароль и получить разрешения администратора. Регулярное архивирование файлов позволит минимизировать ущерб от вирусной атаки;
- Основным средством защиты информации – это резервное копирование ценных данных, которые хранятся на жестких дисках.

Современные антивирусные программы состоят из модулей:

- Эвристический модуль – для выявления неизвестных вирусов.
- Монитор – программа, которая постоянно находится в оперативной памяти ПК.
- Устройство управления, которое осуществляет запуск антивирусных программ и обновление вирусной базы данных и компонентов.
- Почтовая программа (проверяет электронную почту).

- Программа сканер – проверяет, обнаруживает и удаляет фиксированный набор известных вирусов в памяти, файлах и системных областях дисков.
- Сетевой экран – защита от хакерских атак.

К наиболее эффективным и популярным антивирусным программам относятся: Антивирус Касперского 7.0, AVAST, Norton AntiVirus и многие другие.

Вопросы

1. Что такое безопасность информационной системы?
2. Перечислите источники угроз безопасности информационных систем.
3. Назовите основные направления утечки информации.
4. Что относится к средствам защиты информации?
5. Перечислите средства защиты информации от несанкционированного доступа.
6. Какие средства защиты как правило применяются в локальных компьютерных сетях?
7. Что такое криптографическая защита информации?
8. Что такое электронная цифровая подпись?
9. Что такое компьютерный вирус и способы их классификации.
10. Перечислите способы защиты от компьютерных вирусов.