Защита информации

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;
- на 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 защита информации от несанкционированного доступа

Получение доступа к ресурсам информационной системы предусматривает выполнение трех процедур: идентификация, аутентификация и 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. Для шифрования используется алгоритм или устройство, которое реализует определенный алгоритм. Управление шифрованием осуществляется с помощью изменяющегося кода ключа.

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.

Другими словами 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.

Вирусы. Антивирусное программное обеспечение

Компьютерный вирус - программа способная самопроизвольно внедряться и внедрять свои копии в другие программы, файлы, системные области компьютера и в вычислительные сети, с целью создания всевозможных помех работе на компьютере.

Признаки заражения:

- прекращение работы или неправильная работа ранее функционировавших программ
- медленная работа компьютера
- невозможность загрузки ОС
- исчезновение файлов и каталогов или искажение их содержимого
- изменение размеров файлов и их времени модификации
- уменьшение размера оперативной памяти
- непредусмотренные сообщения, изображения и звуковые сигналы
- частые сбои и зависания компьютера и др.

Классификация компьютерных вирусов

По среде обитания:

- *Сетевые* – распространяются по различным компьютерным сетям
- *Файловые* – внедряются в исполняемые модули (COM, EXE)
- *Загрузочные* – внедряются в загрузочные сектора диска или сектора, содержащие программу загрузки диска
- *Фалово-загрузочные* – внедряются и в загрузочные сектора и в исполняемые модули

По способу заражения:

- *Резидентные* – при заражении оставляет в оперативной памяти компьютера свою резидентную часть, которая потом перехватывает обращения ОС к объектам заражения
- *Нерезидентные* – не заражают оперативную память и активны ограниченное время

По воздействию:

- *Неопасные* – не мешают работе компьютера, но уменьшают объем свободной оперативной памяти и памяти на дисках
- Опасные – приводят к различным нарушениям в работе компьютера
- Очень опасные – могут приводить к потере программ, данных, стиранию информации в системных областях дисков

По особенностям алгоритма заражения:

- *Паразиты* – изменяют содержимое файлов и секторов, легко обнаруживаются
- *Черви* – вычисляют адреса сетевых компьютеров и отправляют по ним свои копии

- *Стелсы* – перехватывают обращение ОС к пораженным файлам и секторам и подставляют вместо них чистые области
- *Мутанты* – содержат алгоритм шифровки-дешифровки, ни одна из копий не похожа на другую
- *Трояны* – не способны к самораспространению, но маскируясь под полезную, разрушают загрузочный сектор и файловую систему

Основные меры по защите от вирусов

- оснастите свой компьютер одной из современных антивирусных программ: Doctor Weber, Norton Antivirus, AVP
- постоянно обновляйте антивирусные базы
- делайте архивные копии ценной для Вас информации (гибкие диски, CD)

Классификация антивирусного программного обеспечения

- Сканеры (детекторы). Принцип работы антивирусных сканеров основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов.
- Мониторы. Это целый класс антивирусов, которые постоянно находятся в оперативной памяти компьютера и отслеживают все подозрительные действия, выполняемые другими программами. С помощью монитора можно остановить распространение вируса на самой ранней стадии.
- Ревизоры. Программы-ревизоры первоначально запоминают в специальных файлах образы главной загрузочной записи, загрузочных секторов логических дисков, информацию о структуре каталогов, иногда - объем установленной оперативной памяти. Программы-ревизоры первоначально запоминают в специальных файлах образы главной загрузочной записи, загрузочных секторов логических дисков, информацию о структуре каталогов, иногда - объем установленной оперативной памяти. Для определения