Организация компьютерной безопасности и защита информации

автор: Чекашова Ирина 10А
учитель: Антонова Е.П.

2011 год

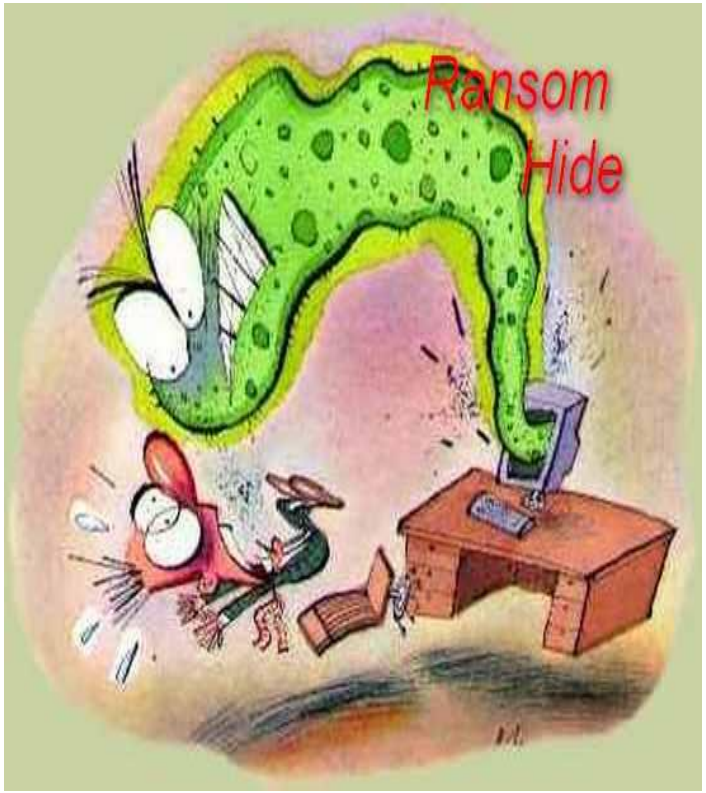
Безопасность информационной системы

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

Источники угроз и их классификация

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.



Защита информации

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.

Средства защиты информации

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

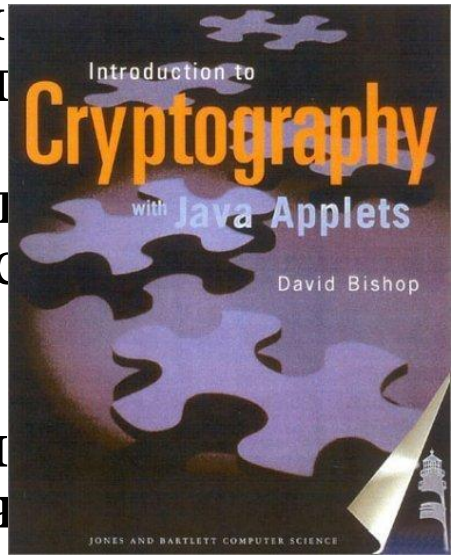
- **Идентификация** - присвоение пользователю (объекту или субъекту ресурсов) уникальных имен и кодов.
- **Аутентификация** - установление подлинности пользователя, представившего идентификатор или проверка того, что лицо или устройство, сообщившее идентификатор является действительно тем, за кого оно 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 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 крипто шифрования используется алгоритм или которое реализует определенный алгорит Управление шифрованием осуществляет помощью изменяющегося кода ключа.



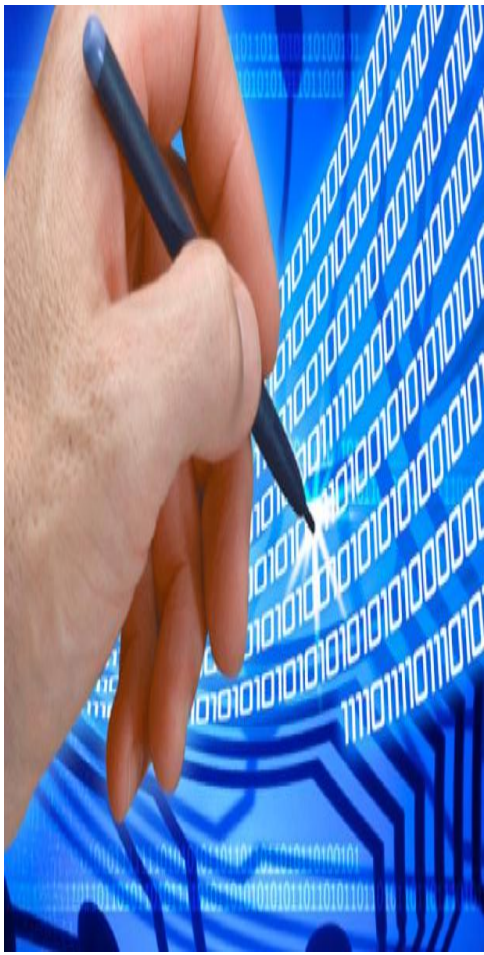
Извлечь зашифрованную информацию м с помощью ключа. Криптография - это оч эффективный метод, который повышает безопасность передачи данных в компьютерных сетях и при обмене информацией между удаленными компьютерами.

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.



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.
В зависимости от среды обитания основными типами компьютерных вирусов являются:

- Программные (поражают файлы с расширением .COM и .EXE) вирусы
- Загрузочные вирусы
- Макровирусы
- Сетевые вирусы
  Источниками вирусного заражения могут быть съемные носители и системы телекоммуникаций.