Защита информации

Цифровая информация – информация, хранение, передача и обработка которой осуществляется средствами ИКТ.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации

Угроза утечки

Виды угроз для цифровой информации

Угроза разрушения

Задания

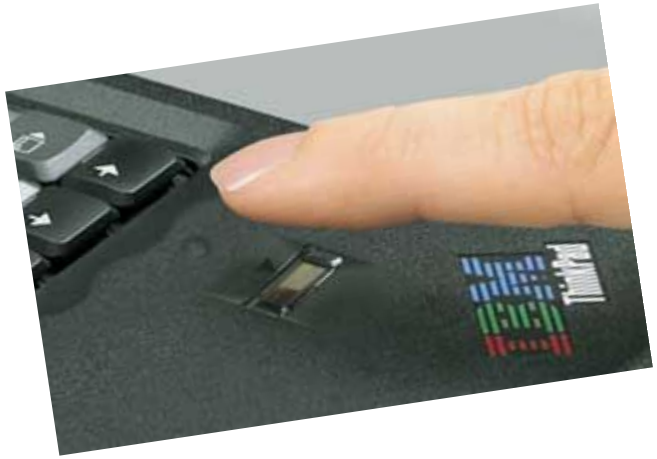
Угроза утечки

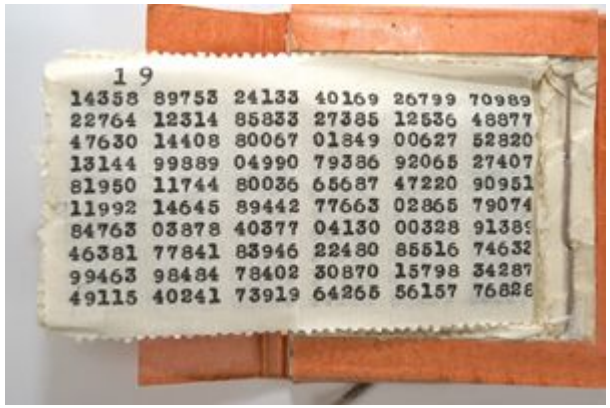
Преднамеренная кража, копирование, прослушивание и пр.

1. **Проникновение в память компьютера, в базы данных ИС**
2. **Перехват в каналах передачи данных, искажение, подлог данных.**

Меры защиты информации

- Физическая защита каналов;
- Криптографические шифры;
- Цифровая подпись и сертификаты.





Криптография

Криптогра´фия (от др.-греч. κρυπτός — скрытый и γράφω — пишу) — наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним), целостности данных (невозможности незаметного изменения информации), аутентификации (проверки подлинности авторства или иных свойств объекта), а также невозможности отказа от авторства.

Материал из Википедии

В криптографической терминологии исходное послание именуют **открытым текстом** (**plaintext** или **cleartext**).

Изменение исходного текста так, чтобы скрыть от прочих его содержание, называют **шифрованием** (**encryption**).

Зашифрованное сообщение называют **шифротекстом** (**ciphertext**).

Процесс, при котором из шифротекста извлекается открытый текст называют **дешифровкой** (**decryption**).

Обычно в процессе шифровки и дешифровки используется некий **ключ** (**key**) и алгоритм обеспечивает, что дешифрование можно сделать лишь зная этот ключ.

Цифровые подписи и сертификаты

Цифровой подписью называют блок данных, сгенерированный с использованием некоторого секретного ключа. При этом с помощью открытого ключа можно проверить, что данные были действительно сгенерированы с помощью этого секретного ключа. Алгоритм генерации цифровой подписи должен обеспечивать, чтобы было невозможно без секретного ключа создать подпись, которая при проверке окажется правильной.

Цифровой сертификат - это сообщение, подписанное полномочным органом сертификации, который подтверждает, что открытый ключ действительно относится к владельцу подписи и может быть использован для дешифрования.

Угроза разрушения

-
  -
  -
-
  -
  -
  -
  -

Меры защиты информации

- Антивирусные программы;
- Брандмауэры;
- Межсетевые экраны

- Резервное копирование;
- Использование ИБП;
- Контроль и профилактика оборудования;
- Разграничение доступа

Вопросы для обсуждения:

- Почему информацию надо защищать?
- Какие основные виды угроз существуют для цифровой информации?
- Какой антивирусной программой Вы пользуетесь?
- Что надо делать, чтобы быть спокойным за информацию на своем личном ПК?
- Какие меры компьютерной безопасности следует использовать в школьном компьютерном классе?
- Какую функцию выполняют брандмауэры и сетевые экраны?
- От чего спасает цифровая подпись?

Защита информации

Задание 1

С помощью справочной системы текстового редактора, установленного на вашем компьютере, выясните:

- можно ли установить пароль на документы, создаваемые в редакторе;
- можно ли изменить атрибуты файлов и сделать их доступными только для чтения.

Если эти операции допустимы, проделайте их.

Задание 2

Сравните, что общего и в чём различие следующих информационных процессов:

- кодирование и декодирование;
- шифрование и «взлом» шифра.

Объясните, насколько возможна автоматизация этих процессов и чем обуславливается эта возможность.

Интернет-источники

- https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F
- http://algolist.manual.ru/defence/intro.php
- https://www.pgpru.com/biblioteka/osnovy/vvedenievkripto/glava1/kriptosotkrytymkljuchom
- http://bgconsulting.ru/news/65/ - рисунок папки с ключом
- http://www.bytemag.ru/articles/detail.php?ID=6719 - *Владислав Шаров* Биометрические методы компьютерной безопасности 13.04.2005 (картинка)