§12. Защита информации.

Рыженко Е. В.
МБОУ г. Астрахани " СОШ №64"

Потеря

Сохранность

Защищаемая информация

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

ГОСТ основных терминов и определений в области защиты информации. 1997г.

Собственник

- частное лицо – *автор*

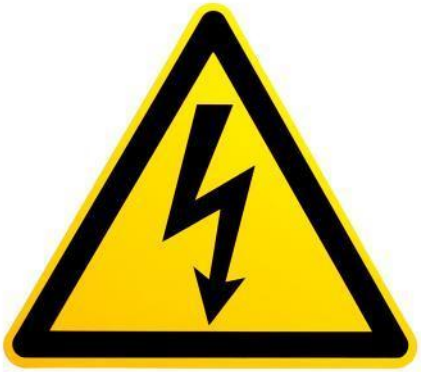
- группа лиц - *авторск*
  группа

- юридическое лицо –
  официально
  зарегистрированная
  организация

- государство

Цифровая информация

- информация, хранение, передача и обработка которой осуществляются средствами ИКТ.



ВИДЫ УГРОЗ ДЛЯ ЦИФРОВОЙ ИНФОРМАЦИИ

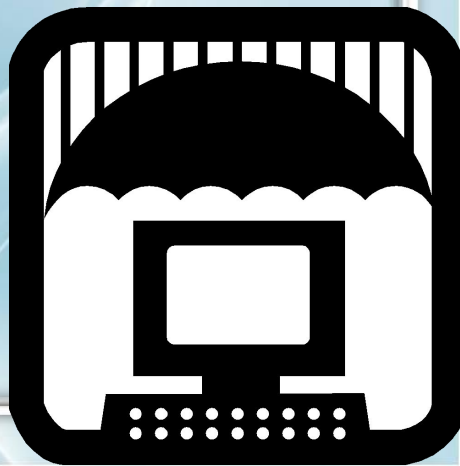
1) кража или утечка информации;

2) разрушение, уничтожение информации.

Защита информации

- деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

ГОСТ основных терминов и определений в области защиты информации. 1997г.



Утечка информации

- представляет собой кражу или копирование бумажных или цифровых документов, прослушивание телефонных разговоров, кража с помощью компьютерной сети и пр. в интересах:

- частных лиц;
- конкурирующих организаций;
- СМИ;
- государственных структур:
  - внешней разведки;
  - служб безопасности.

Несанкционированное воздействие

- это преднамеренная порча или уничтожение информации, а также информационного оборудования со стороны лиц, не имеющих на это права (санкции).

К этой категории деятельности относится

- Создание и распространение компьютерных вирусов;
- Хакерская деятельность;
- Физическое воздействие на аппаратное обеспечение.

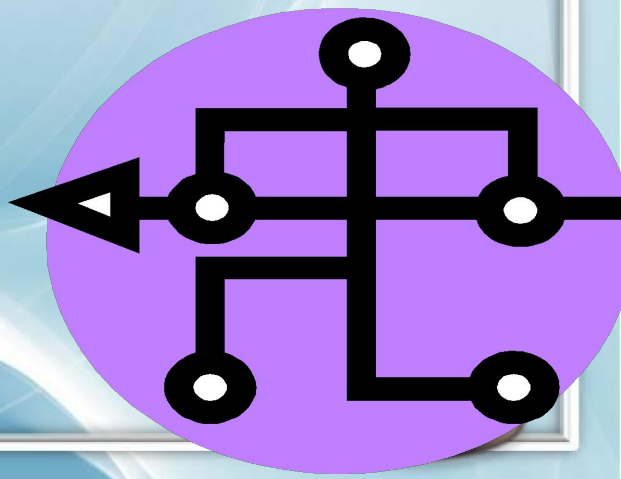
Компьютерный вирус

- вредоносный программный код, способный нанести ущерб данным на компьютере или вывести его из строя.

«Трояны» – вирусы-шпионы, внедрившись в ОС компьютера тайно пересылает заинтересованным лицам конфиденциальную информацию.

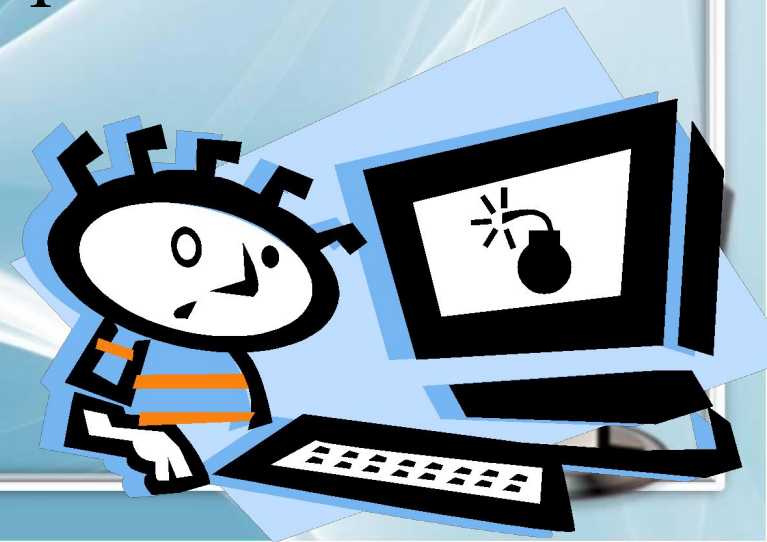
Хакерская атака

- это одновременное обращение с большого количества компьютеров на сервер информационной системы. Сервер не справляется с таким валом запросов, что приводит к «зависанию» в его работе.



Непреднамеренное воздействие

- ошибки пользователя;
- сбой в работе оборудования и программного обеспечения;
- авария электросети;
- пожар, землетрясение и пр.



Правила безопасности

- ✔ периодически осуществлять ***резервное копирование***: файлы с наиболее важными данными дублировать и сохранять на внешних носителях;
- ✔ регулярно осуществлять ***антивирусную проверку*** компьютера;
- ✔ использовать ***блок бесперебойного питания;***

Правила безопасности

- ✔ организовать ***разграничение доступа*** для разных пользователей ПК;
- ✔ использовать защитные программы - ***брандмауэры, межсетевые экраны***.

Системы шифрования
(криптография)

Ключ – определяет алгоритм шифрования:

- **с закрытым ключом,** которым заранее обмениваются два абонента, ведущие секретную переписку, и сохраняемый в тайне от третьих лиц.
- **с открытым ключом** (асимметричный алгоритм), использует отдельно шифровальный (открытый) и дешифровальный (закрытый) ключей.

Цифровая подпись

- это индивидуальный секретный шифр, ключ которого известен только владельцу.

- закрытый ключ применяется для шифрования;
- открытый – для дешифрования.

Цифровой сертификат

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

Вопросы:

- Почему информацию надо защищать?
- Какие основные виды угроз существуют для цифровой информации?
- Встречались ли вы со случаями поражения вирусами? Какой антивирусной программой вы пользуетесь?
- Что такое хакерская атака? Для кого она опасна?
- Что надо делать, чтобы быть спокойным за информацию в своём личном ПК?
- Какие меры компьютерной безопасности следует использовать в школьном компьютерном классе?
- Чем отличается шифрование с закрытым ключом от шифрования с открытым ключом?
- Какую функцию выполняют брандмауэры и сетевые экраны?
- От чего спасает цифровая подпись?

Домашнее задание:

1. Какой вариант ключа Цезаря использован для шифрования тайнописи: ТУНЫИО, ЦЕЛЖЗО,ТСДЗЖЛО! Расшифруйте.
2. Попробуйте расшифровать сообщение: BYAJHVFNBRF-K.,BVSQ GHTLVTN DCT[EXTYBRJD!

(подсказка: ключ связан с расположением знаков на клавиатуре)

1. Зашифруйте тем же методом фразу:

ВСЁ ТАЙНОЕ СТАНОВИТСЯ ЯВНЫМ.

Источники информации:

- Информатика и ИКТ. Базовый уровень. 10-11кл.Семакин И. Г., Хеннер Е. К., Москва. Бином. Лаборатория знаний. 2012.
- контент сайта Office.com
- http://im5-tub-ru.yandex.net/i?id=34018642-41-72&n=21
- http://im4-tub-ru.yandex.net/i?id=161222788-60-72&n=21
- http://im7-tub-ru.yandex.net/i?id=74662593-13-72&n=21