Информационная безопасность. Защита цифровых данных. Криптография

Защищаемая информация*

- * Это информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации. Всякая информация является чьей-то собственностью, как и материальная собственность.
- *Цифровая информация* – информация, хранение, передача и обработка которой осуществляются средствами ИКТ.
- *Защита информации* – деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Виды угроз для цифровой информации

Утечка информации – кража или копирование бумажных документов, прослушивание телефонных разговоров, распространение цифровых носителей для хранения данных.

Например:

- проникновение в память компьютера, в базы данных информационных систем;
- Перехват в каналах передачи данных;
- Искажение, подлог данных.

Меры защиты информации

Основные 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** (ББП).

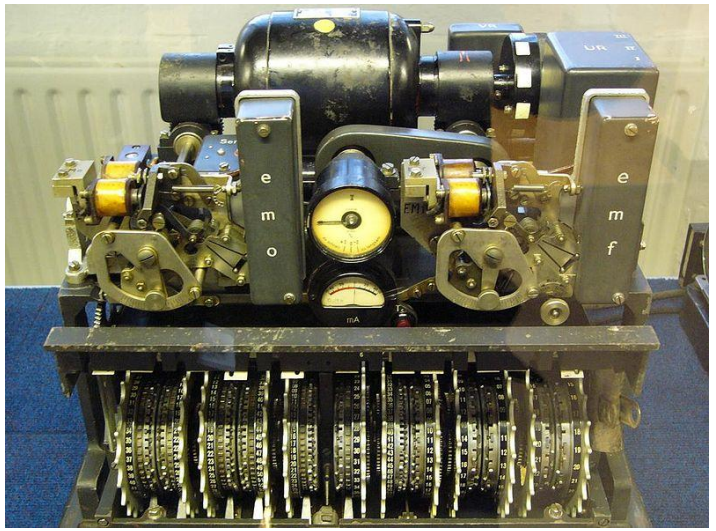
Защитные программы – брандмауэры.

Межсетевые экраны – брандмауэры, защищающие сети, подключенные к другим сетям.

Криптография и защита информации

- *Криптография* - наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства, а также невозможности отказа от авторства) информации.
- *Закрытый ключ* – ключ, которым заранее обмениваются два абонента, ведущие секретную переписку. Это единый ключ, с помощью которого происходит как шифрование, так и дешифрование.

Немецкая криптомашина, которая использовалась во время Второй Мировой Войны.



Цифровые подписи и сертификаты

- *Цифровая подпись* – индивидуальный секретный шифр, ключ которого известен только владельцу. Закрытый ключ применяется для шифрования, а открытый – для дешифрования.
- *Цифровой сертификат* – сообщение, подписанное полномочным органом сертификации, который подтверждает, что открытый ключ действительно относится к владельцу подписи и может быть использован для дешифрования.