**Методы защиты информации. Криптография. Аутентификация. Цифровая подпись.**

Методы защиты:

1. Криптографические метода – шифрование информации и эл. подпись
2. Программные и технические методы – программные: средства управления доступом и аудит, имеющиеся в ОС; технич.: замки в дверях, система видеонаблюдения, камеры, сигнализация
3. Методич. средства – это различные законодательные нормативные документы, которые определяют правила доступа и работы с инф-ей, а т же санкции за их нарушения.

Криптография

чтобы никто посторонний не мог ознакомиться с передаваемым сообщением М, А некоторым образом преобразует сообщение в форму недоступную для прочтения посторонних. С=Ек(М). И преобразует так обратное сообщение направляется дальше. В выпо-ет обратное преобразование и восстанавливает из него исх. сообщение М. М=Dк(С).

Исходное сообщение наз-ся открытым текстом, независимо от типа его содержания. Преобразованное сообщения С наз-ся шифр-текстом.

Процесс преобраз-ся открытого текста в шифртекст наз-ся **шифрование**. Обратный процесс – расшифрование.

Параметр К – ключ для заш-я, расш-я.

Наука, изучающая методы защиты сооб-ий наз-мя криптографией, м-ды вскрытия текста – криптоанализом.

Преобразование открытого текста в шифртекст заключается в вычислении некоторой ф-ции от открытого текста.

Процесс расшифрования заключается в применении к шифр-тексту обратной ф-ции расшифрования.

Совокупность функций расшифрования и шифрования называется **криптографическим алгоритмом или шифром**.

Надежность любого современного шифра основывается на использованиии ключа. Знание функции расшифрования и шифрования является недостаточным для раскрытия сообщения - **принцип Кирхгофа**.

Если в шифре ключ расшифрования совпадает с ключом шифрования или может быть из него получен, тогда шифр называется **симметричным**.

Если ключ расшифрования (личный) практически невозможно получить из ключа шифрования (открытый), то шифр называется шифром с открытым ключом.

**Шифры**:

1. Блочные(инф обраб-ся блоками фиксир длины, длина блока от 64 бит)
2. Потоковые(инф обраб-ся потоком, побитно или побайтно)

Установление подлинности объекта **(аутентификация)** - методика, которая позволяет одной стороне доказывать подлинность другой стороны. Объект может быть человеком, процессом, клиентом или сервером. **Объект, подлинность которого должна быть доказана, называется претендентом;** признаки подлинности (идентификационный код) претендента названы **верификатором**.

**Категории проверки**

В установлении подлинности объекта претендент должен идентифицировать себя для верификатора. Это может быть сделано одним из трех видов свидетелей: нечто, известное только претенденту , нечто, чем обладает только претендент, или нечто, свойственное только претенденту.

- **Нечто известное**. Это - секретная информация известная только претенденту, что может быть проверено верификатором. Примеры: пароль, PIN-код, ключ засекречивания и секретный ключ.

**- Нечто, чем обладает**. Это то, что может доказать опознавательный код претендента. Примеры: паспорт, водительские права, удостоверение личности, кредитная карточка и карточка с интегральной схемой, включающей микропроцессор.

- **Нечто свойственное**. Это свойственные претенденту характеристики. Примеры: обычные подписи, отпечатки пальца, голос, характеристики лица, образец сетчатки глаза и почерк.

Аутентификация бывает **односторонней** (обычно клиент доказывает свою подлинность серверу) и **двусторонней** (**взаимной**). Пример односторонней аутентификации - процедура входа пользователя в систему.

**Электронная подпись** (ЭП) — информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Электронная подпись предназначена для идентификации лица, подписавшего электронный документ и является полноценной заменой (аналогом) собственноручной подписи в случаях, предусмотренных законом.

Использование электронной подписи позволяет осуществить:

- Контроль целостности передаваемого документа;

- Защиту от изменений (подделки) документа;

- Невозможность отказа от авторства.