Презентация на тему “Защита информации”

Выполнила ученица 10 класса Нагаева К.

План презентации:

- Что такое защита информации?
- Виды угроз цифровой иформации
- Меры защиты информации
- Криптография и защита информации
- Цифровые подписи и сертификаты

Что такое защита информации

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

Виды угроз для цифровой информации

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

Можно различить два основных вида угроз цифровой информации:

1. Кража или утечка информации
2. Разрушение, уничтожение информации

В ГОСТЕ дается следующее определение защиты информации:

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

Утечка информации происходила и в “докомпьютерные” времена. Она представляет собой кражу или копирование бумажных документов, прослушивание телефонных разговоров и пр. С распространением цифровых носителей для хранения данных они так же становятся объектами краж.

С развитием компьютерных сетей появился новый канал утечки – кража через сети. Заинтересованными в такой утечке могут быть отдельные лица, конкурирующие организации в бизнесе, СМИ, государственные структуры: внешняя разведка или службы безопасности.

Разрушение информации может быть несанкционированным и непреднамеренным. В чем различие?

Несанкционированное воздействие – это преднамеренная порча или уничтожение информации со стороны лиц, не имеющих на это права. К этой категории угроз относится деятельность людей, занимающихся созданием и распространением *компьютерных вирусов*. Так же существуют *вирусы-шпионы*.

Непреднамеренное воздействие происходит вследствие ошибок пользователя, а также из-за сбоев в работе оборудования или ПО. В конце концов могут возникнуть и непредвиденные внешние факторы: авария электросети, пожар или землетрясение и пр.

Меры защиты информации

Основные правила безопасности, которые следует соблюдать для защиты информации:

- Переодически осуществлять **резервное копирование**: файлы с наиболее важными данными дублировать и сохранять на внешних носителях
- Регулярно осуществлять **антивирусную проверку** компьютера
- Использовать **блок бесперебойного питания**

Блок бесперебойного питания (ББП) осуществляет защиту данных при отключении электроэнергии или скачка напряжения в сети.

Антивирусные программы занимаются борьбой с сотнями компьютерных вирусов из Всемирной паутины.

Разграничение доступа для разных пользователей ПК существует для защиты информации от доступа посторонних людей.

Брандмауэр – защитные программы для безопасного пользования Интернетом.

Криптография и защита информации

Криптография - наука о методах обеспечения конфиденциальности, целостности данных, аутентификации, а также невозможности отказа от авторства. Простым языком – это тайнопись.

Древнеримский император Юлий Цезарь придумал шифр, носящий название **шифра Цезаря**. Во время разных войн тайнопись использовалась для донесений.

С развитием компьютерных коммуникаций, “старая” криптография снова стала актуальной. Существующие методы шифрования делятся на методы с закрытым ключом и методы с открытым ключом. Ключ определяет алгоритм дешифровки.

Закрытый ключ - это ключ, которым заранее обмениваются два абонента, ведущие секретную переписку. Основная задача: сохранить ключ в тайне от третьих лиц.

Алгоритмы с **открытым ключом ,** или **ассиметричные алгоритмы,** базируются на использовании отдельных шифровального и дешифровального ключей. В алгоритмах с открытым ключом требуется, чтобы закрытый ключ невозможно было вычислить по открытому. Исходя из этого требования, шифровальный ключ может быть доступным кому угодно без какого-либо ущерба безопасности для алгоритма шифрования.

Цифровые подписи и сертификаты

Цифровая подпись – это индивидуальный секретный шифр, ключ которого известен только владельцу.

Наличие цифровой подписи свидетельствует о том, что ее владелец подтвердил подлинность содержимого переданного сообщения.

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

Чтобы получить сертификат полномочного органа сертификации , нужно представить в этот орган документы, подтверждающие личность заявителя.