**9 класс 28.04.**

**Тема урока Защита информации.**

В наше время все большая часть информации хранится в цифровом виде, на компьютерных носителях. Оказывается, это обстоятельство не упрощает, а усложняет проблему защиты информации.

Причем эта проблема принимает настолько глобальный характер, что государством принимаются специальные законы о защите информации, создаются новые службы, которых не было раньше.

В 1997 году Госстандартом России разработан ГОСТ основных терминов и определений в области защиты информации. В этом документе дано следующее понятие защищаемой информации: ***защищаемая******информация*** *– информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.*

Главная мысль определения состоит в том, что всякая информация является чьей- то собственностью, как и материальная собственность. Поэтому защита информации государственными законами рассматривается как защита собственности. Собственником информации может быть частное лицо, группа лиц, юридическое лицо, т.е. официально зарегистрированная организация.

*Виды угроз для цифровой информации.*

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

Можно различить *два основных вида угроз для цифровой информации:*

* 1. кража и *утечка информации*
  2. *разрушение*, уничтожение *информации*

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

*Утечка информации* – представляет собой *кражу информации*  или копирование бумажных документов, прослушивание телефонных разговоров. С развитием компьютерных сетей появился новый канал утечки - кража через сети. Если компьютер подключен к глобальной сети, то он потенциально доступен для проникновения в его информационную базу извне. В такой утечке информации заинтересованы конкретные лица, например СМИ, конкурирующие организации, хакеры очень часто любят взламывать различные базы данных. Развившаяся за последние десятилетия телефонная сотовая связь также не лишена этих проблем. По мнению специалистов, невозможно со стопроцентной гарантией обеспечить безопасность в этой сфере. Согласно данным примерам *разрушение информации может быть несанкционированным и непреднамеренным.* различие между этими воздействиями, в чем же различие? Попробуем разобраться. ***Несанкционированное воздействие*** *– это преднамеренная порча или уничтожение информации, а также информационного оборудования со стороны лиц, не имеющих на это права (санкции*). К этой категории угроз относится деятельность людей, занимающихся созданием и распространением компьютерных *вирусов – вредоносных программных кодов, способных нанести ущерб данным на компьютере или вывести его из строя.*

Кроме вирусов разрушителей существуют еще вирусы - шпионы. Их называют *троянцами*. Внедрившись в операционную систему вашего компьютера, такой троянец может тайно от вас пересылать заинтересованным лицам вашу конфиденциальную информацию.

К несанкционированному вмешательству относится криминальная деятельность так называемых хакеров – «взломщиков» информационных систем с целью воздействия на их содержание и работоспособность. Например, чтобы снять деньги с чужого счета. Большой вред корпоративным информационным системам наносят так называемые хакерские атаки. *Хакерская атака – это одновременное обращение большого количества компьютеров на сервер информационной системы*. Сервер не справляется с таким валом запросов, что приводит к «зависанию» в его работе.

*Непреднамеренное воздействие происходит вследствие ошибок пользователя, а также из-за сбоев в работе оборудования или программного обеспечения.* А также потеря информации может произойти из-за внешних факторов: пожары, наводнения, землетрясения.

**Меры защиты информации**

Принимаемые для защиты информации меры в первую очередь зависят от уровня ее использования, от значимости информации и степени ущерба, который может нанести владельцу ее утечка или разрушение.

Основные правила безопасности, которые необходимо соблюдать:

* Периодически осуществлять ***резервное копирование***: *файлы с наиболее важными данными дублировать и сохранять на внешних носителях;*
* Регулярно осуществлять ***антивирусную проверку компьютера***;
* Использовать ***блок бесперебойного питания.***
* Защитой от форс-мажорных ситуаций являются блоки бесперебойного питания.

Основным разносчиком вирусов является нелицензионное программное обеспечение, файлы, скопированные из случайных источников, а также службы Интернета: электронная почта. Борьбой с вирусами занимаются создатели антивирусных программ, которые регулярно необходимо обновлять. Если один и тот же компьютер используется несколькими лицами и личная информация требует защиты от доступа посторонних, то с помощью системных средств организуется *разграничение прав доступа для разных пользователей – создание учетной записи, то есть создается логин и пароль.* Наибольшим опасностям подвергаются пользователи глобальных сетей, Интернета. Для защиты компьютеров, подключенных к сети, от подозрительных объектов, «кочующих» по сети, используются защитные программы, которые называются ***брандмауэрами*** (*защитные программы, которые помогают отражать атаки хакеров, червей и вирусов, пытающихся попасть на компьютер через Интернет*). Критерии подозрительности может определять сам брандмауэр или задавать пользователь. *Брандмауэры, защищающие сети называют* ***межсетевыми экранами***. Утечка информации может происходить путем перехвата в процессе передачи информации по каналам связи. Если от этого не удается защититься с помощью технических средств, на помощь приходят системы шифрования. *Методами шифрования занимается криптография*. С развитием компьютерных коммуникаций, старая криптография снова стала актуальной. Существующие методы шифрования делятся на методы с закрытым ключом и метода с открытым ключом. Ключ определяет алгоритм дешифровки*. Закрытый ключ – 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 отдельного шифровального (открытого) или дешифровального (закрытого) ключей.

**Цифровые подписи и сертификаты.**

Методы криптографии позволяют осуществлять не только засекречивание сообщений. Существуют приемы защиты целостности сообщения, позволяющие обнаружить факты изменения или подмены текста, а также подлинности источника сообщения.

Недавно появилась технология *цифровой подписи – это индивидуальный секретный шифр, ключ которого известен только владельцу.* Наличие цифровой подписи свидетельствует о том, что ее владелец подтвердил подлинность содержимого переданного сообщения.

Если вы получили документ с цифровой подписью, то вам нужен открытый ключ, для расшифровки, но как узнать тот ли ключ вы получили. Здесь в дело вступают цифровые сертификаты. *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 данный сертификат необходимо предоставить документы, подтверждающие личность заявителя.

**Написать в тетрадь конспект. Проверю потом тетрадь!!!!!!**