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

Собственником информации может быть частное лицо (например, автор), группа лиц (авторская группа), юридическое лицо, т. е. официально зарегистрированная организация. Наконец, существует государственная собственность на определенную информацию.

Виды угроз для цифровой информации

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

Можно различить два основных вида 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.

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, для снятия денег с чужого счета в банке, для уничтожения данных следственных органов и пр. Большой вред корпоративным информационным системам наносят так называемые хакерские атаки. *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 происходит вследствие ошибок пользователя, а также из-за сбоев в работе оборудования или программного обеспечения. В конце концов, могут возникнуть и непредвиденные внешние факторы: авария электросети, пожар или землетрясение и пр.

Меры защиты информации

Если речь идет о персональной информации отдельного пользователя ПК, то главной опасностью является потеря данных по непреднамеренным причинам, а также из-за проникновения вредоносных вирусов.

Основные правила безопасности, которые следует соблюдать, такие:

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

Одной из часто случающихся форс-мажорных (внезапных, непреодолимых) ситуаций является отключение электроэнергии или скачки напряжения в сети. Если компьютер от этого не защищен, то можно потерять не только данные, но и сам компьютер: какие-то его части могут выйти из строя. Защитой от этого являются блоки бесперебойного питания (ББП). Обязательно подключайте ваш ПК к электросети через ББП.

Проблема антивирусной защиты компьютера очень злободневна. Основным разносчиком вирусов является нелицензионное программное обеспечение, файлы, скопированные из случайных источников, а также службы Интернета: электронная почта, Всемирная паутина — WWW. Каждый день в мире появляются сотни новых компьютерных вирусов. Борьбой с этим злом занимаются специалисты, создающие антивирусные программы. Лицензионные антивирусные программы следует покупать у фирм-производителей. Однако антивирусную программу недостаточно лишь однажды установить на компьютер. После этого нужно регулярно обновлять ее базу — добавлять настройки на новые типы вирусов. Наиболее оперативно такое обновление производится

через Интернет серверами фирм-производителей.

Если один и тот же компьютер используется многими лицами и личная информация каждого требует защиты от доступа посторонних, то с помощью системных средств организуется разграничение доступа для разных пользователей ПК. Для этого создаются учетные записи пользователей, устанавливаются пароли на доступ к информации, для зашифрованной информации создаются конфиденциальные ключи дешифрования. Меры разграничения доступа обязательно используются на сетевых серверах.

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. Критерии подозрительности может определять сам брандмауэр или задавать пользователь. Например, пользователь может запретить прием посланий по электронной почте с определенных адресов или определенного содержания. Брандмауэры могут предотвращать атаки, фильтровать ненужные рекламные рассылки и прочее. Брандмауэры, защищающие сети, подключенные к другим сетям, называются межсетевыми экранами.

Утечка информации может происходить путем перехвата в процессе передачи по каналам связи. Если от этого не удается защититься техническими средствами, то применяют системы шифрования. Методами шифрования занимается криптография.

Криптография и защита информации

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. Это единый ключ, с помощью которого происходит как шифрование, так и дешифрование. Основная задача секретной переписки — сохранить ключ в тайне от третьих лиц.

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.

Сравнительно недавно появилась технология цифровой подписи, благодаря чему исчезла необходимость передавать подписанный подлинник документа только в бумажном виде. Разумеется, здесь речь не идет о сканировании подписи.

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

методах цифровой подписи часто используются алгоритмы шифрования с открытым ключом, но несколько иначе, чем обычно, а именно: закрытый ключ применяется для шифрования, а открытый — для дешифрования.

Наличие цифровой подписи свидетельствует о том, что ее владелец подтвердил подлинность содержимого переданного сообщения.
Если вы получили документ, заверенный цифровой подписью, то вам нужен открытый ключ для ее расшифровки, переданный владельцем подписи. И вот тут скрывается проблема: как удостовериться, что открытый ключ, который вы получили, действительно является ключом владельца? 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 сертификат полномочного органа сертификации, нужно представить в этот орган документы, подтверждающие личность заявителя.

Система основных понятий

<table>
<tr><td colspan="4">Защита цифровой информации</td></tr>
<tr><td colspan="4">Цифровая информация - информация, хранение, передача и обработка которой осуществляются средствами ИКТ</td></tr>
<tr><td colspan="4">Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.</td></tr>
<tr><td colspan="2">Угроза утечки</td><td colspan="2">Угроза разрушения</td></tr>
<tr><td colspan="2">Преднамеренная кража, копирование, прослушивание и пр.</td><td>Несанкционированное разрушение</td><td>Непреднамеренное разрушение</td></tr>
<tr><td>Проникновение в память компьютера, в базы данных информационных систем</td><td>Перехват в каналах передачи данных, искажение, подлог данных</td><td>Вредоносные программные коды-вирусы; деятельность хакеров, атаки</td><td>Ошибки пользователя, сбои оборудования, ошибки и сбои в работе ПО, форс-мажорные обстоятельства</td></tr>
<tr><td colspan="4">Меры защиты информации</td></tr>
<tr><td colspan="2">Физическая защита каналов; криптографические шифры; цифровая подпись и сертификаты</td><td>Антивирусные программы; брандмауэры; межсетевые экраны</td><td>Резервное копирование; использование ББП; контроль и профилактика оборудования; разграничение доступа</td></tr>
</table>