ЗАЩИТА ИНФОРМАЦИИ

Основные термины и определения

(ГОСТ Р 50922-96 ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ. Защита информации. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ)

Цифровая информация - информация, хранение, передача и обработка которой осуществляется средствами ИКТ.

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

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

Виды угроз для цифровой информации

Различают два основных вида угроз для цифровой информации:

1. **кража или утечка информации;**
2. **разрушение, уничтожение информации.**

Разрушение информации может быть *несанкционированным* и *непреднамеренным*.

Несанкционированное воздействие – 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 вирусы-шпионы. Их называют *троянцами.*

К несанкционированному вмешательству относится криминальная деятельность хакеров – « взломщиков» информационных систем с целью воздействия на их содержание и работоспособность.

Большой вред наносят хакерские атаки. Атака – 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, программного обеспечения, аварии электросети, пожара и т.д.

Угроза утечки

Преднамеренная кража, копирование, прослушивание и пр.

Проникновение в память компьютера, в базы данных информационных систем	**Перехват в каналах передачи данных, искажение, подлог данных**

Угроза разрушения	
Несанкционированное разрушение	**Непреднамеренное разрушение**
Вредоносные программные коды-вирусы; деятельность хакеров, атаки	**Ошибки пользователя, сбои оборудования, ошибки и сбои в работе ПО, форс-мажорные обстоятельства**

Меры защиты

Угроза утечки	Угроза разрушения	
Физическая защита каналов; криптографические шифры; цифровая подпись и сертификаты	Антивирусные программы; брандмауэры; межсетевые экраны	Резервное копирование; использование ББП; контроль и профилактика оборудования; разграничение доступа


Методы защиты информации
Шифрование (криптография) информации
Законодательные меры
Ограничение доступа к информации
Преобразование (кодирование) слов и т.д. с помощью специальных алгоритмов
Контроль доступа к аппаратуре
Вся аппаратура закрыта и в местах доступа к ней установлены датчики, которые срабатывают при вскрытии аппаратуры
На уровне среды обитания человека: выдача документов, установка сигнализации или системы видеонаблюдения
На уровне защиты компьютерных систем: введение паролей для пользователей

Меры защиты персональной информации отдельного пользователя:

- 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).**

Меры защиты компьютеров, подключённых к сети:

- использование защитных программ - **брандмауэров;**
- физическая защита каналов;
- использование криптографических шифров (существующие методы шифрования делятся на методы с закрытым ключом и методы с открытым ключом; ключ определяет алгоритм дешифрования);
- использование цифровых подписей и сертификатов.*

*__Цифровая подпись –__ индивидуальный секретный шифр, ключ которого известен только владельцу.

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

Правовые методы защиты информации в компьютерных системах

1. Конституция РФ, статьи 2, 23, 24;
2. Федеральный закон РФ «Об информации, информатизации и защите информации». Принят 25 мая 1995г.;
3. Федеральный закон РФ «О безопасности». Принят 25 декабря 1992г.

4. Статья 272 УК РФ «Неправомерный доступ к компьютерной информации»;
5. Статья 273 УК РФ «Создание, использование и распространение вредоносных программ для ЭВМ», части 1,2;
6. Статья 274 УК РФ «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети», части 1,2;
7. Статья 138 УК РФ «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений»;
8. Статья 201 УК РФ «Злоупотребление полномочий»

Контрольные вопросы