Защита от несанкционированного доступа к информации. Способы защиты информации.

- ***Доступ к информации*** **- ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.**

- ***Несанкционированный доступ к информации*** **(НСД) - доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.**

В защите информации ПК от НСД можно выделить три основных направления:

- первое ориентируется на недопущение нарушителя к вычислительной среде и основывается на специальных технических средствах опознавания пользователя;
- второе связано с защитой вычислительной среды и используются различные программные методы по защите информации;
- третье направление связано с использованием специальных средств защиты информации ПК от несанкционированного доступа.

1.Специальные технические средства опознавания пользователя

Самыми распространёнными техническими средствами являются – *биометрические системы идентификации*.

К биометрическим системам относятся системы идентификации:

- по отпечаткам пальцев;
- по характеристикам речи;
- по радужной оболочке глаза;
- по изображению лица;
- по геометрии ладони руки.

2. Программные методы по защите информации

Стандартные программные средства защиты:

а) средства защиты вычислительных ресурсов, использующие парольную идентификацию;

б) применение различных методов шифрования информации;

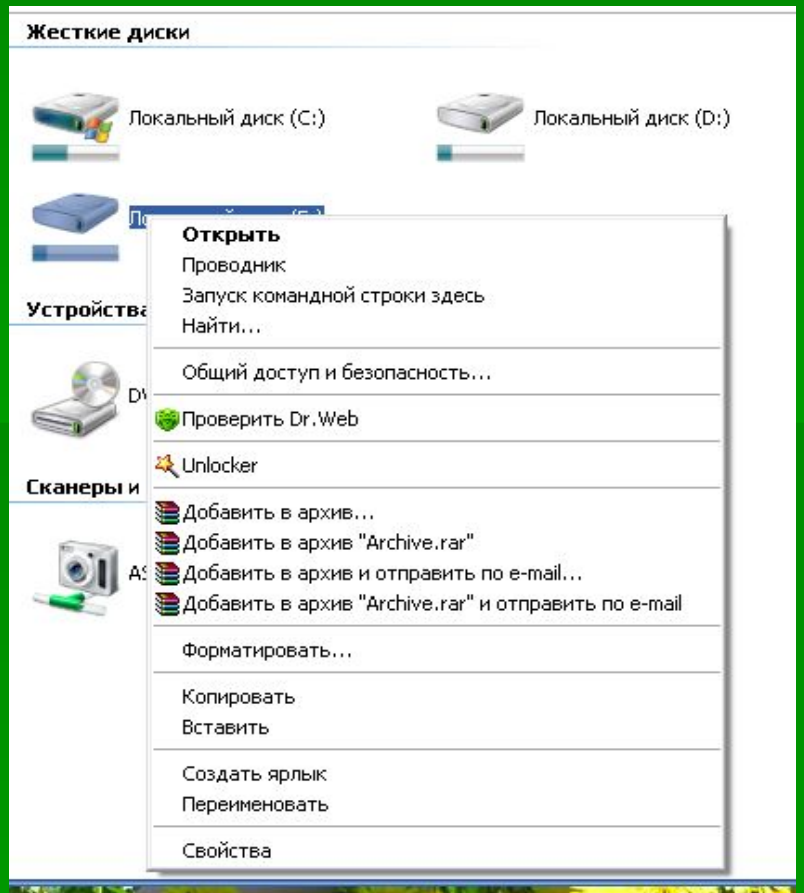
в) средства защиты от копирования коммерческих программных продуктов;

г) защита от компьютерных вирусов.

а) пароли можно установить:

- в программе BIOS (компьютер не начинает загрузку ОС, если не введён правильный пароль (стр.44, рис.1.15), но возникнут проблемы если пользователь забудет пароль);
- при загрузке операционной системы (каждый пользователь при загрузке ОС должен ввести свой пароль (стр.44, рис.1.16));

- пароль можно установить на каждый диск, папку или файл (для них могут быть установлены определённые права доступа, причём права могут быть различными для разных пользователей – команда «Общий доступ и безопасность» в контекстном меню))



б) применение различных методов шифрования

Самой надежной защитой от несанкционированного доступа к передаваемой информации через локальные сети и к программным продуктам ПК является применение различных методов шифрования (криптографических методов защиты информации).

Данный метод защиты реализуется в виде программ или пакетов программ, расширяющих возможности стандартной операционной системы.

Криптографические методы защиты информации - это специальные методы шифрования, кодирования или иного преобразования информации, в результате которого ее содержание становится недоступным без предъявления ключа криптограммы и обратного преобразования.

Четыре основные группы шифрования символов:

- ***подстановка*** - символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее определенным правилом;
- ***перестановка*** - символы шифруемого текста переставляются по некоторому правилу в пределах заданного блока передаваемого текста;
- ***аналитическое преобразование*** - шифруемый текст преобразуется по некоторому аналитическому правилу;
- ***комбинированное преобразование*** - исходный текст шифруется двумя или большим числом способов шифрования.

в) средства защиты от копирования коммерческих программных продуктов

- установка условной метки или характеристики, которая была присуща данному носителю, не воспроизводиться любыми средствами копирования;
- диск имеет ряд уникальных характеристик, присущих только одному диску, и эти характеристики теряются при копировании на другой диск (т.е. когда диск спокойно можно копировать, и распространять его содержимое, но старт будет производиться только при наличии оригинального диска);
- уникальный код (ключ) на установку лицензионного программного обеспечения.

3.Специальные средства защиты информации ПК

Электронные ключи (HASP или Sentinel) **подключаются практически ко всем портам компьютера: от LPT до USB, а также слотам ISA и PCI, при возникновении такой необходимости.**

Основой ключей HASP является специализированная заказная микросхема, имеющая уникальный для каждого ключа алгоритм работы.

II. Правовая защита конфиденциальной информации и ответственность за неправомерные действия в отношении этой информации.

Защита конфиденциальной информации от неправомерных посягательств осуществляется на основе норм гражданского, административного либо уголовного права.

ГК РФ

- **ст.150:** относит конфиденциальную информацию к нематериальным благам ;
- **ст.11ч.1:** предусматривает судебную защиту гражданских прав. Защиту нарушенных или оспоренных гражданских прав, согласно этой статье осуществляет в соответствии с подведомственностью дел, установленной процессуальным законодательством, суд, арбитражный суд или третейский суд;
- **ст.12:** определены способы защиты гражданских прав, большинство которых могут применяться в связи с защитой конфиденциальной информации.

УК РФ

Ст.137: предусматривает ответственность за правонарушения, связанные с нарушением права на защиту конфиденциальной информации. В ней определена ответственность (***наказывается штрафом или исправительными работами)*** за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений;

- **Ст.138**: предусматривает, что это же деяние, совершенное лицом с использованием своего служебного положения или специальных технических средств, предназначенных для негласного получения информации, наказывается штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью.

Кодекс АП

- **статьей 13.12** предусмотрена ответственность за нарушение правил защиты информации. Так, нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), влечет наложение административного штрафа;
- **статья 13.14** устанавливает, что за разглашение информации, доступ к которой ограничен федеральным законом, лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, влечет наложение административного штрафа.