

ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ

Информатика, 11 класс

ЗАЩИТА С ИСПОЛЬЗОВАНИЕМ ПАРОЛЕЙ

Для защиты от несанкционированного доступа к программам и данным, хранящимся на компьютере, используются *пароли*.

Вход по паролю может быть установлен в программе BIOS Setup, компьютер не начнет загрузку операционной системы, если не введен правильный пароль.

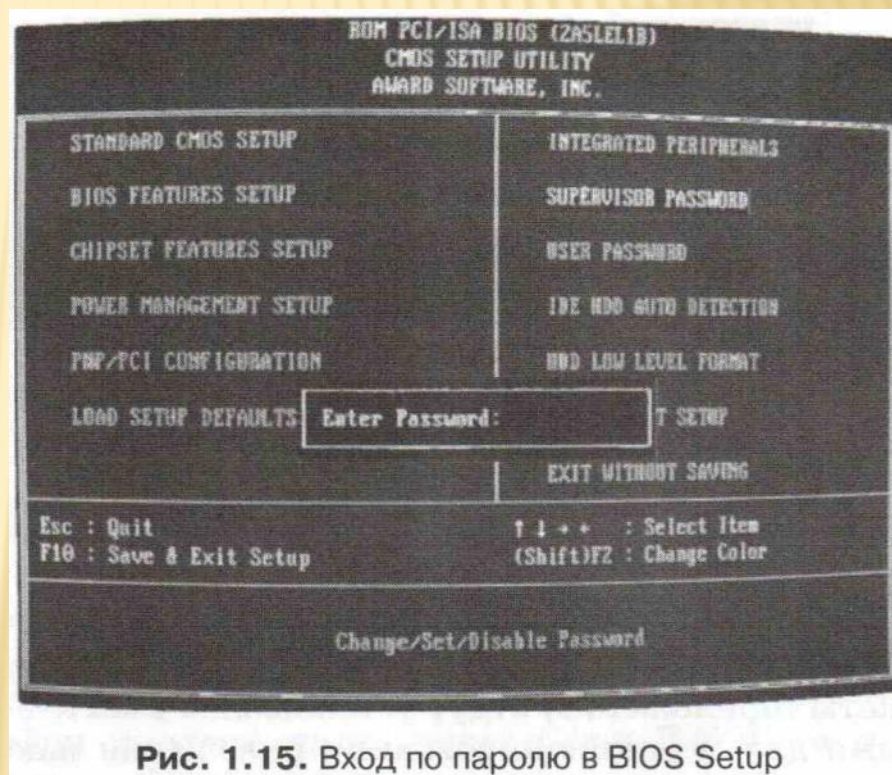


Рис. 1.15. Вход по паролю в BIOS Setup

Защита с использованием пароля используется при загрузке операционной системы (при загрузке системы каждый пользователь должен ввести свой пароль).

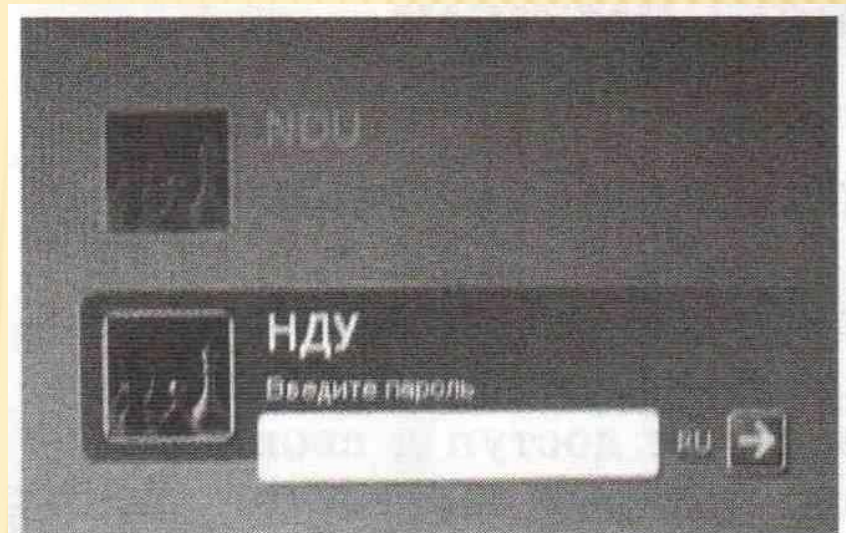


Рис. 1.16-1. Ввод пароля в операционной системе Windows

От несанкционированного доступа может быть защищен каждый диск, папка или файл локального компьютера. Для них могут быть установлены определенные права доступа (полный доступ, изменение, чтение, запись и др.), причем права могут быть различными для различных пользователей.

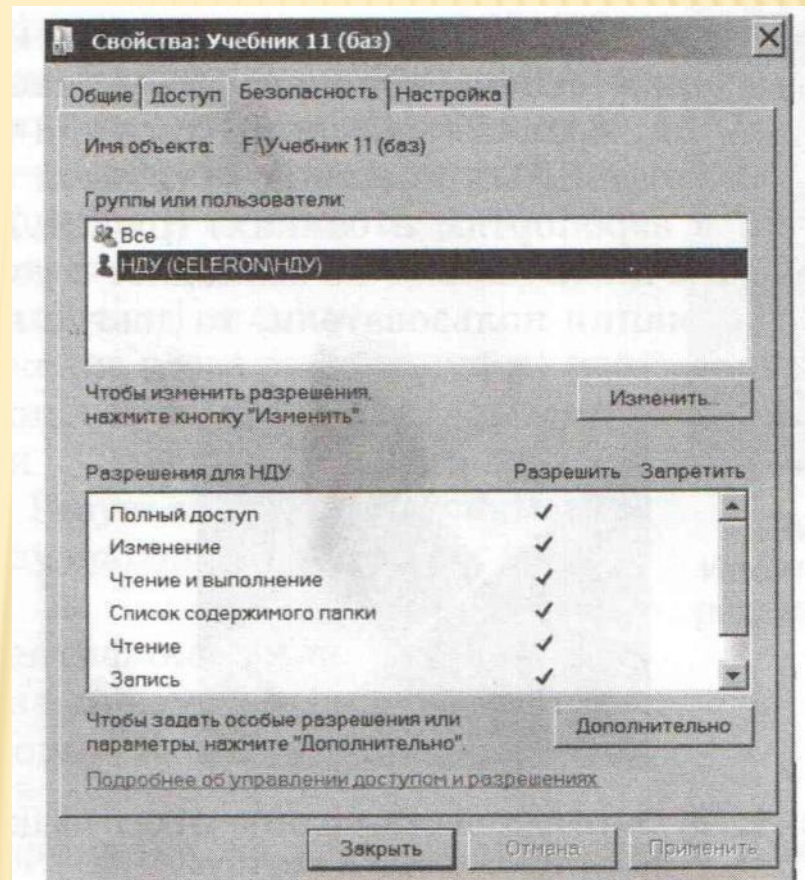


Рис. 1.17. Установка прав доступа к папке в операционной системе Windows

БИОМЕТРИЧЕСКИЕ СИСТЕМЫ ЗАЩИТЫ

В настоящее время для защиты от несанкционированного доступа к информации все более часто используют **биометрические системы идентификации**. Используемые в этих системах характеристики являются неотъемлемыми качествами личности человека и поэтому не могут быть утраченными и подделанными. К биометрическим системам защиты информации относятся системы идентификации:

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

ИДЕНТИФИКАЦИЯ ПО ОТПЕЧАТКАМ ПАЛЬЦЕВ

Оптические сканеры считывания отпечатков пальцев устанавливаются на ноутбуки, мыши, клавиатуры, флэш-диски, а также применяются в виде отдельных внешних устройств и терминалов.

Если узор отпечатка пальца не совпадает с узором допущенного к информации пользователя, то доступ к информации невозможен.



Оптический сканер отпечатка пальца, вмонтированный в ноутбук

ИДЕНТИФИКАЦИЯ ПО ХАРАКТЕРИСТИКАМ РЕЧИ

Идентификация человека по голосу – один из традиционных способов распознавания, интерес к этому методу связан и с прогнозами внедрения голосовых интерфейсов в операционные системы. Голосовая идентификация бесконтактна и существуют системы ограничения доступа к информации на основании частотного анализа речи.

Каждому человеку присуща индивидуальная частотная характеристика каждого звука (фонемы).



Рис. 1.19. Голосовая идентификация по частотной характеристике речи

ИДЕНТИФИКАЦИЯ ПО РАДУЖНОЙ ОБОЛОЧКЕ ГЛАЗА

Радужная оболочка глаза является уникальной для каждого человека биометрической характеристикой. Она формируется в первые полтора года жизни и остается практически неизменной в течение всей жизни.

Изображение глаза выделяется из изображения лица и на него накладывается специальная маска штрих-кодов. Результатом является матрица, индивидуальная для каждого человека.

Для идентификации по радужной оболочке глаза применяются специальные сканеры, подключенные к компьютеру.

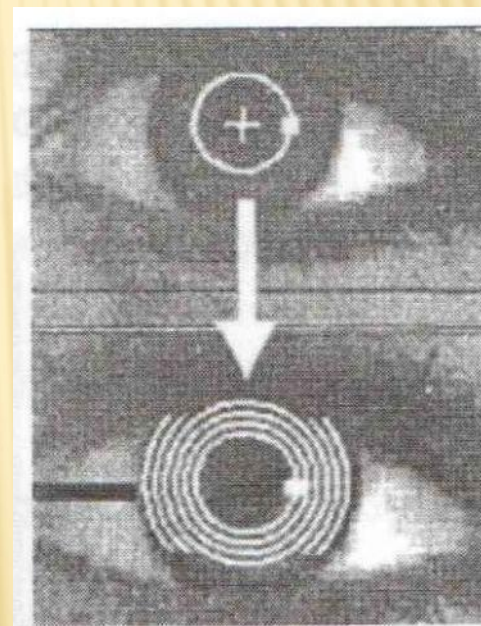


Рис. 1.20.
Идентификация по
радужной оболочке
глаза

ИДЕНТИФИКАЦИЯ ПО ИЗОБРАЖЕНИЮ ЛИЦА

Для идентификации личности часто используются технологии распознавания по лицу. Они ненавязчивы, так как распознавание человека происходит на расстоянии, без задержек и отвлечения внимания и не ограничивают пользователя в свободе перемещений.

По лицу человека можно узнать его историю, симпатии и антипатии, болезни, эмоциональное состояние, чувства и намерения по отношению к окружающим. Всё это представляет особый интерес для автоматического распознавания лиц (например, для выявления потенциальных преступников).

Идентификационные признаки учитывают форму лица, его цвет, а также цвет волос. К важным признакам можно отнести также координаты точек лица в местах, соответствующих смене контраста (брови, глаза, нос, уши, рот и овал).

В настоящее время начинается выдача новых загранпаспортов, в микросхеме которых хранится цифровая фотография владельца.

ИДЕНТИФИКАЦИЯ ПО ЛАДОНИ РУКИ

В биометрике в целях идентификации используется простая геометрия руки – размеры и форма, а также некоторые информационные знаки на тыльной стороне руки (образы на сгибах между фалангами пальцев, узоры расположения кровеносных сосудов).

Сканеры идентификации по ладони руки установлены в некоторых аэропортах, банках и на атомных электростанциях.

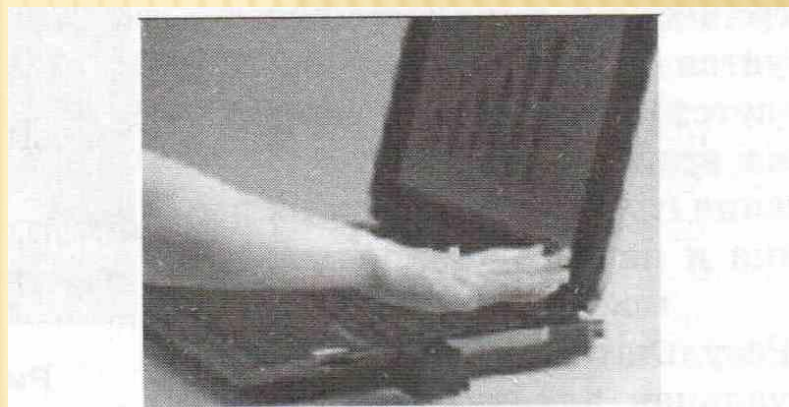


Рис. 1.21. Идентификация по ладони руки

ВОПРОСЫ:

1. Как защищается информация в компьютере с использованием паролей?
2. Какие существуют биометрические методы защиты информации?