

Защита от несанкционированного доступа к информации



Каждый год в мире потери от преднамеренного нанесения вреда ИТ системам компании теряют огромные средства.

В результате компании непрерывного цикла могут пострадать вплоть до банкротства.

Защита с использованием паролей

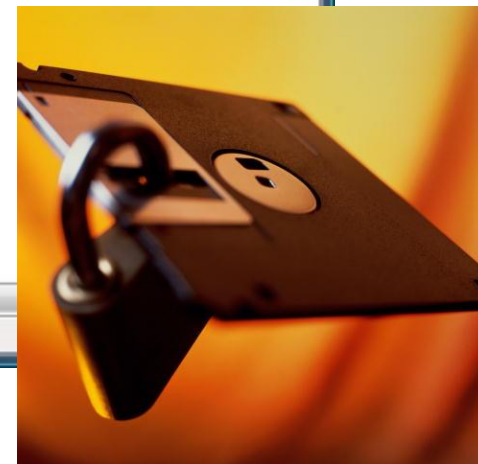
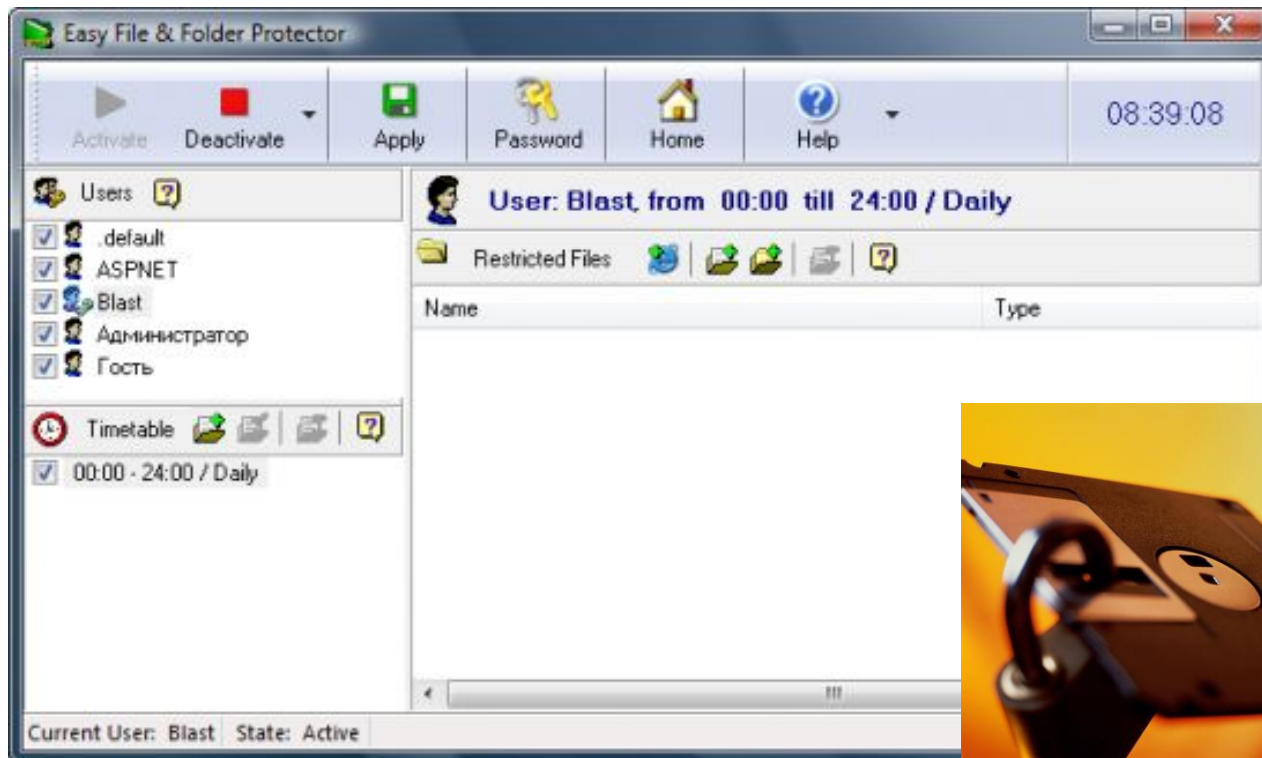
- Для защиты от несанкционированного доступа к программам и данным, хранящимся на компьютере, используются **пароли**.
- Компьютер разрешает доступ к своим ресурсам только тем пользователям, которые зарегистрированы и ввели правильный пароль.
- При этом может производиться регистрация всех попыток несанкционированного доступа.



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



- 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.)



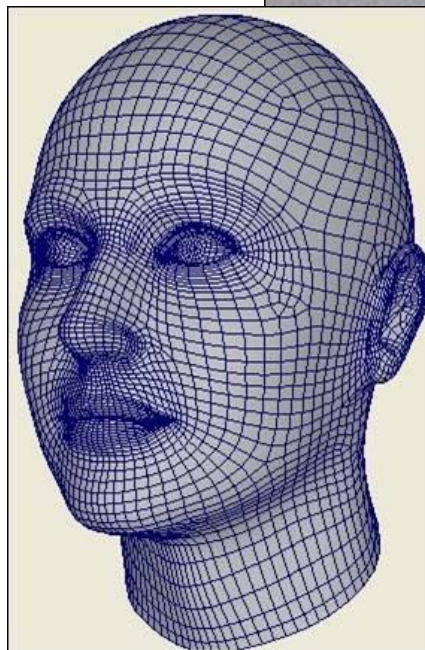
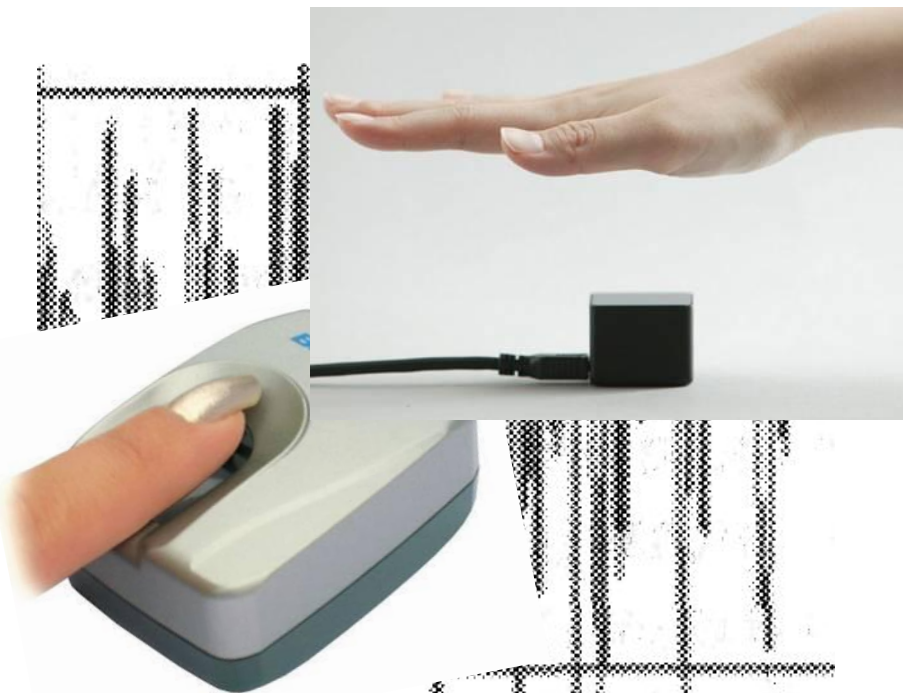
Биометрические системы защиты

- В настоящее время часто используются **биометрические системы идентификации**.
- Используемые в этих системах *характеристики являются неотъемлемыми качествами личности человека* и поэтому не могут быть утерянными 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.



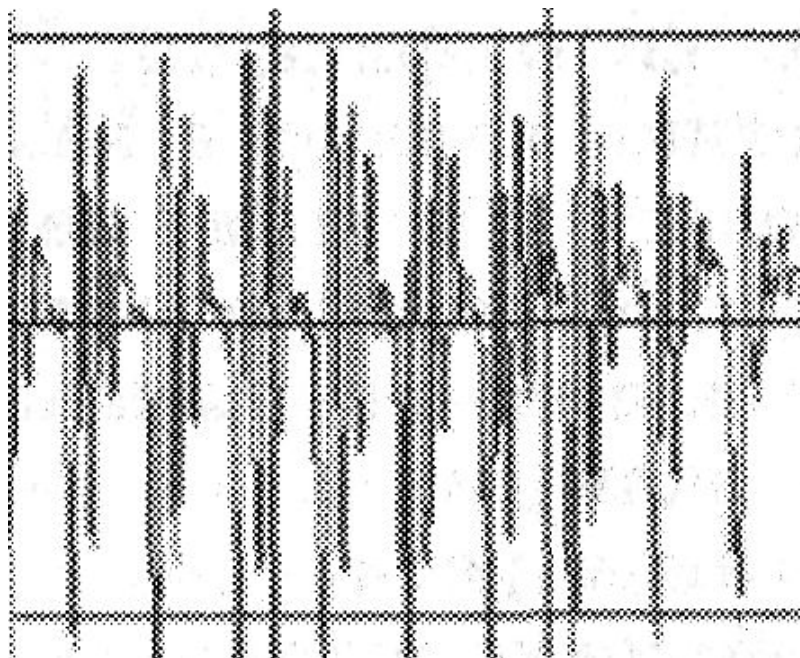
Идентификация по отпечаткам пальцев.

- Оптические сканеры считывания отпечатков пальцев устанавливаются на ноутбуки, мыши, клавиатуры, флэш-диски, а также применяются в виде отдельных внешних устройств и терминалов (например, в аэропортах и банках)
- Если узор отпечатка пальца не совпадает с узором допущенного к информации пользователя, то доступ к информации невозможен.



Идентификация по характеристикам речи.

- Идентификация человека по голосу — один из традиционных способов распознавания. Голосовая идентификация бесконтактна и существуют системы ограничения доступа к информации на основании частотного анализа речи



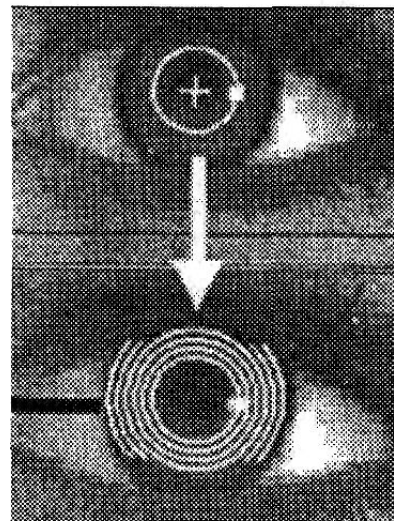
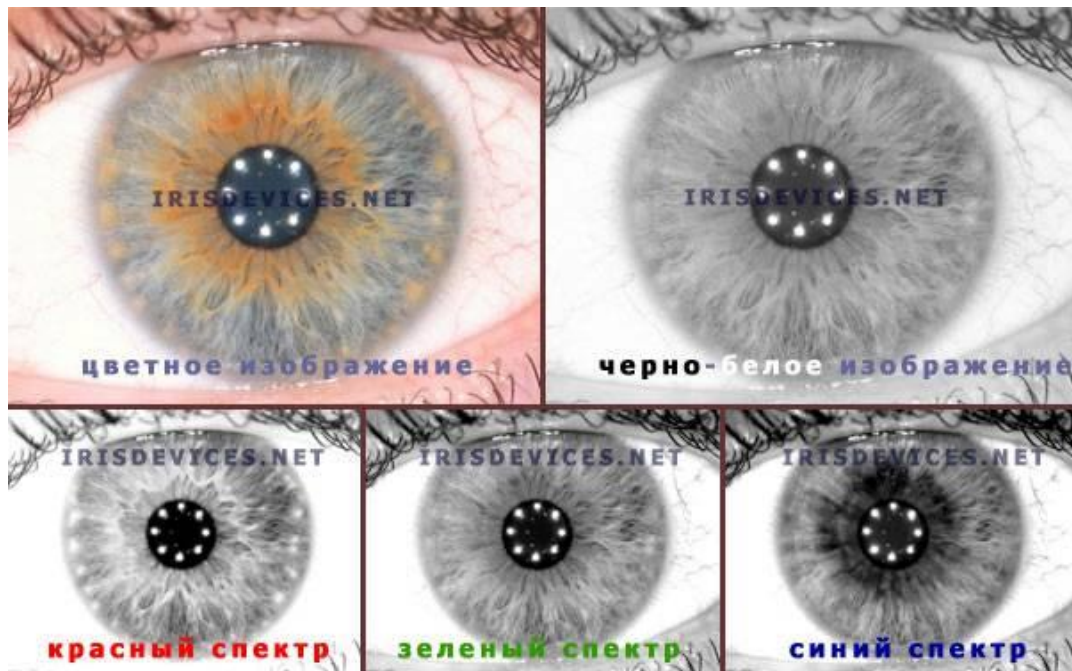
Идентификация по радужной оболочке глаза.

- 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.



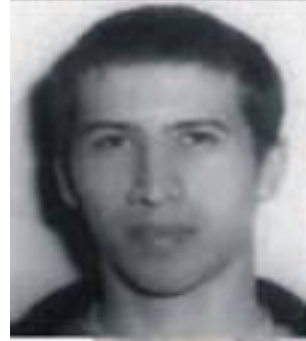
Идентификация по радужной оболочке глаза.

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



Идентификация по изображению лица.

- Для идентификации личности часто используется 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.
- В настоящее время идет 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



- Как защищается информация в компьютере с использованием паролей?
- Какие существуют биометрические методы защиты информации?



Задание на дом: § 1.4

