Тема:Методы защиты информаций

Основные понятия

Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Информационная безопасность – защита целостности, доступности и конфиденциальности информации.

Целостность - актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

доступность- возможность за приемлемое время получить требуемую информационную услугу

Конфиденциальность - защита от несанкционированного доступа к информации.

Информационная безопасность — это состояние защищённости информационной среды.

В вычислительной технике понятие безопасности подразумевает

- надежность работы компьютера,
- сохранность ценных данных,
- защиту информации от внесения в нее изменений неуполномоченными лицами,
- сохранение тайны переписки в электронной связи.

Во всех цивилизованных странах на безопасности граждан стоят законы, для защиты информации используется Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями и дополнениями), но все же надежность работы компьютерных систем во многом опирается на меры самозащиты.

Несанкционированный доступ

Несанкционированный доступ - действия, нарушающ установленный порядок доступа или правила разграничения, дос к программам и данным, который получают абоненты, которые не прошли регистрацию и не имеют права на ознакомление или рабо с этими ресурсами.

Для предотвращения несанкционированного доступа осуществляется контроль доступа.

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.

Каждому конкретному пользователю может быть разрешен доступ только к определенным информационным ресурсам.

При этом может производиться регистрация всех попыток несанкционированного доступа.

Защита с использованием пароля

используется при загрузке операционной системы

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

ащиту

нелегк

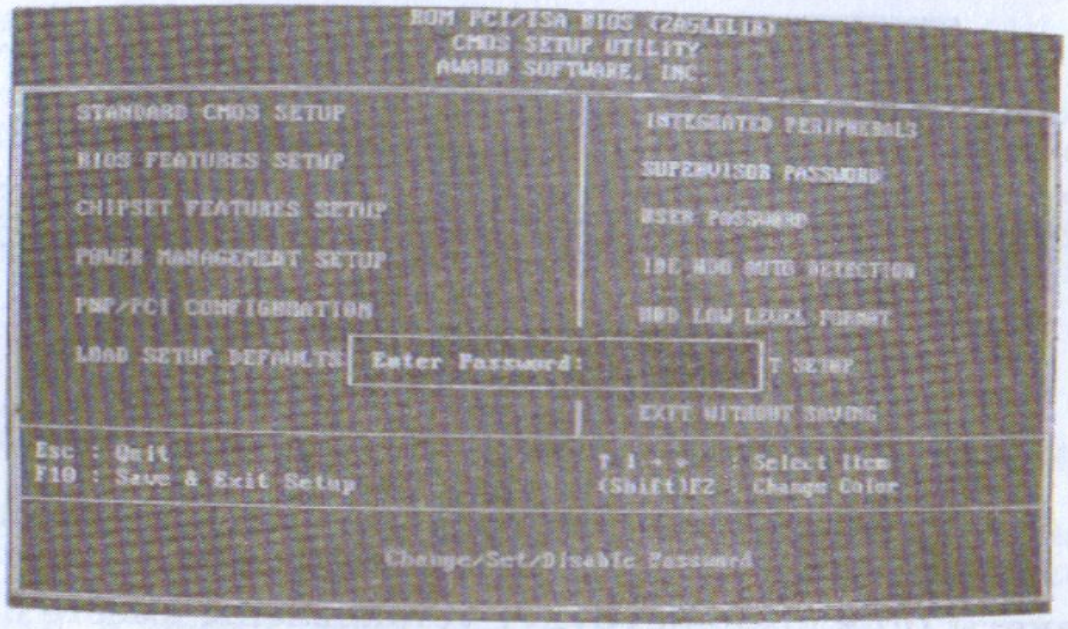


Рис. 1.16. Вход по паролю в BIOS Setup

От несанкционированного доступа может быть защищены

- каждый диск,
- каждая папка,
- каждый файл локального компьютера.

Для них могут быть установлены определенные права доступа

- полный доступ,
- возможность внесения изменений,
- только чтение,
- запись и др.

Права могут быть различными для различных пользователей.

Что такое пароль?

"***пароль*** - это секретный набор различных символов, позволяющий определить ***законного пользователя и его права*** на работу в компьютерной системе".

Общая идея такая: самый лучший пароль - случайный и бессмысленный набор символов.

Храните пароль в надежном месте.

Регулярно меняйте пароли. Это может ввести злоумышленников в заблуждение. Чем надежнее пароль, тем дольше можно его использовать. Пароль из 8 и менее символов можно применять в течении недели, в то время как комбинация из 14 и более символов может служить несколько лет.

Биометрические системы защиты

В настоящее время для защиты от несанкционированного доступа к информации все более часто используются ***биометрические системы идентификации.***

Биометрическая идентификация - это способ идентификации личности по отдельным специфическим биометрическим признакам (идентификаторам), присущим конкретному человеку

Методы биометрической идентификации, делятся на две группы:

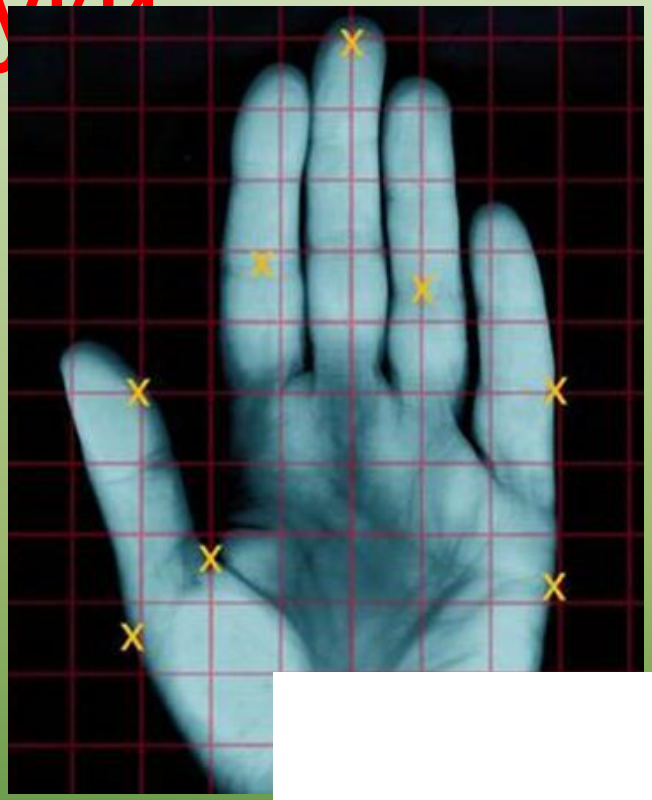
Статические методы	Динамические методы
по отпечаткам пальцев; по геометрии ладони руки	**По рукописному почерку**. Эта технология становится весьма популярной альтернативой росписи ручкой. Анализируются динамические признаки написания — степень нажима, скорость письма
по радужной оболочке глаза; по изображению лица;	**По голосу**. Построения кода идентификации по голосу, как правило, это различные сочетания частотных и статистических характеристик голоса

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.

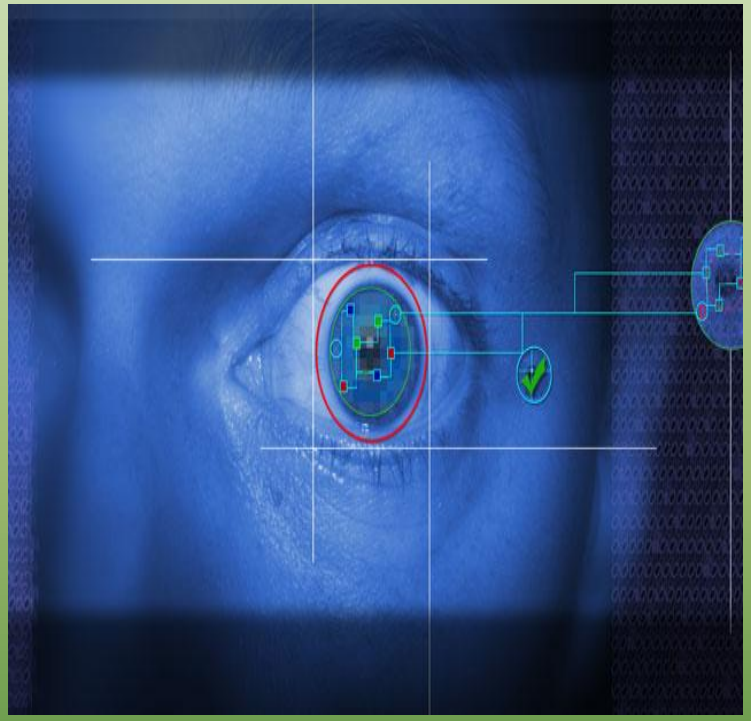
Идентификация по ладони руки



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 .

Идентификация по радужной оболочке глаза



Радужная оболочка глаза является уникальной для каждого человека биометрической характеристикой.

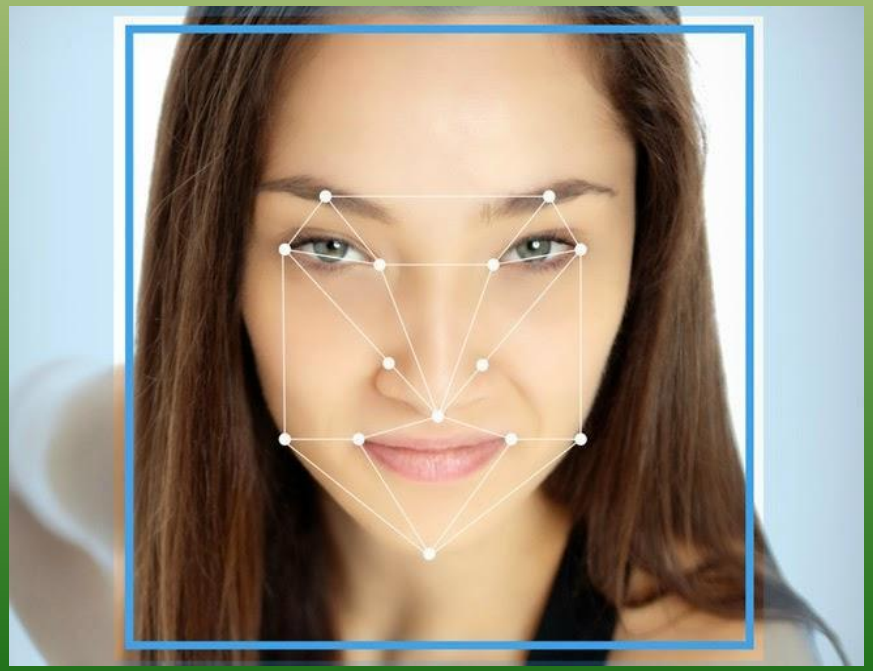
Изображение глаза выделяется из изображения лица и на него накладывается специальная маска штрих - кодов. Результатом являет ся матрица, индивидуальная для каждого

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

Идентификация по изображению лица

Для идентификации личности часто используются технологии распознавания по лицу. Распознавание человека происходит на расстоянии. 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 микро схеме которых хранится цифровая фотография владельца.

До последнего времени считалось, что самый надежный метод биометрической идентификации и аутентификации личности — это метод, основанный на сканировании сетчатки глаза. Он содержит в себе лучшие черты идентификации по радужной оболочке и по венам руки. Сканер считывает рисунок капилляров на поверхности сетчатки глаза. Сетчатка имеет неподвижную структуру, неизменную во времени, кроме как в результате глазной болезни, например, катаракты.

К сожалению, целый ряд трудностей возникает при использовании этого метода биометрии. Сканером тут является весьма сложная оптическая система, а человек должен значительное время не двигаться, пока система наводится, что вызывает неприятные ощущения.

Динамические методы идентификации – по рукописному тексту

ОБЩИЕ ПРИЗНАКИ ПОЧЕРКА,

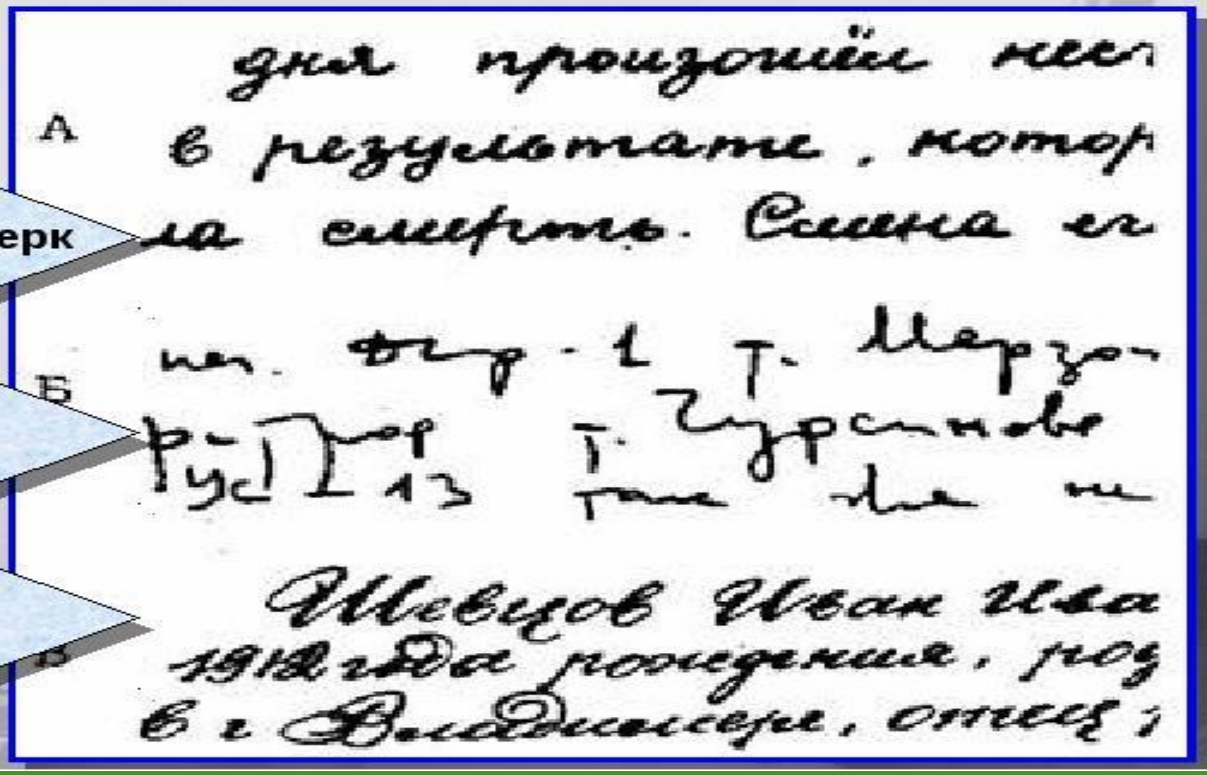
отражающие степень сформированности и характер письменно-двигательного навыка

- Координация движений;
- Темп письма (быстрый медленный средний);
- Сложность движений:

Простой по сложности почерк

Упрощенный почерк

Усложненный почерк



Производители биометрического оборудования пытаются создать надёжные системы идентификации лиц с использованием динамических признаков. Дополнительное аппаратное обеспечение таких систем дешевле, чем сканеры отпечатков пальцев или радужки глаза. Системы идентификации личности по динамике воспроизведения рукописных паролей (подписей) весьма удобны и

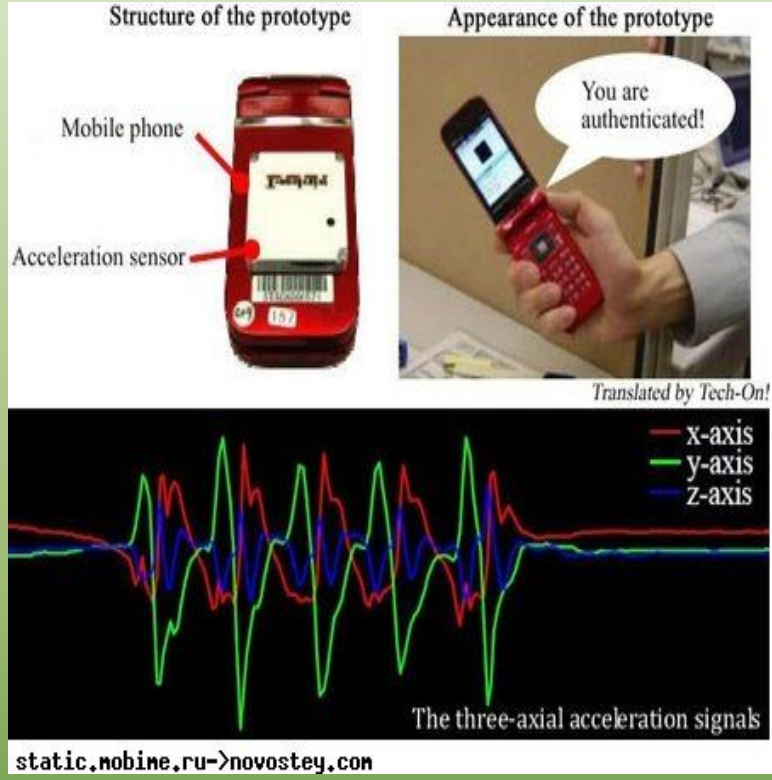
Приборы и стенды лаборатории по исследованию почерка и документов

Универсальный просмотровый детектор DORS 1300

Стенды лаборатории почерковедения

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.

Системы аутентификации по голосу при записи образца и в процессе последующей идентификации опираются на такие уникальные для каждого человека особенности голоса, как высота, модуляция и частота звука. Эти показатели определяются физическими характеристиками голосового тракта и уникальны для

Достоинства биометрических систем идентификации вполне очевидны: уникальные физиологические характеристики человека хороши тем, что их трудно подделать,
например, невозможно оставить фальшивый отпечаток пальца при помощи своего собственного или сделать радужную оболочку своего глаза похожей на чью-то другую.
В отличие от документальных идентификаторов (паспорт, водительские права, удостоверение личности), от пароля или персонального идентификационного номера, биометрические характеристики не могут быть забыты или потеряны.
В силу своей уникальности биометрические признаки используются для предотвращения воровства или мошенничества.
Методы биометрической идентификации постоянно

Угринович Н.Д. Информатика и ИКТ. Учебник для 11 класса. М.: БИНОМ. Лаборатория знаний, 2010. - 188 с.

Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями и дополнениями) Система ГАРАНТ: http://base.garant.ru/12148555/#ixzz3iKhW4RYL

Википедия http://ru.wikipedia.org/

http://jgk.ucoz.ru

http://www.bio-profile.ru/images/Test-Anviz.jpg