**Установление паролей**

Пароль – это секретный набор различных символов, позволяющий определить законного пользователя и его права на работу в компьютерной системе

Пароль может применяться для различных целей:

- определения "свой – чужой";

- подтверждение личности владельца ключевого элемента (например, кредитной или магнитной карточки);

- прав работы в системе и допуска к информации;

- получения специальных прав на выполнение особо важных операций;

- ключ для системы шифрования или электронной подписи и т.д.

От несанкционированного доступа могут быть защищены:

* каждая папка;
* каждый диск;
* 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.

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 правильный пароль. Преодолеть такую защиту нелегко.

Какой пароль выбрать?

1. пароль не должен легко раскрываться, подбор пароля должен быть максимально затруднен. В основе пароля не должно лежать ваше имя, дата рождения, кличка любимой кошки и т.п.

2. в Windows лучше всего защищены от взлома пароли длиной 7 или 14 знаков; кроме того, рекомендуется использовать в пароле сочетание букв, цифр и специальных символов (таких как подчерк, решетка, доллар, собака и т.п.), причем желательно, чтобы хотя бы один из этих символов присутствовал среди знаков пароля со второго по шестой.

3. рекомендуется использовать в паролях и строчные, и прописные буквы, причем примерно поровну и вперемешку.

Личные номера на сегодняшний день являются одним из наименее безопасных паролей широкого использования (напр. Кредитные карты для кассовых аппаратов АТМ или телефонные карты). В личных номерах могут использоваться цифры от 0 до 9, то есть номер может иметь десять тысяч вариаций. Этого достаточно если речь идет о человеке стоящем возле АТМ и набирающего код наугад, но совсем не много если речь идет о компьютере использующем лобовой метод решения.

Но большинство компьютерных паролей длиннее и кроме чисел 1-9 могут содержать символы. Четырехразрядный пароль, в котором используются числа и символы, расшифровать сложнее – он может содержать 1679616 уникальных комбинаций.

**Биометрические системы защиты информации**

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

Используемые в этих системах характеристики являются неотъемлемыми качествами личности человека и поэтому не могут быть утерянными и подделанными.

Обычно при классификации биометрических технологий выделяют две группы систем по типу используемых биометрических параметров:

• Первая группа систем использует статические биометрические параметры: отпечатки пальцев, геометрия руки, радужная оболочка глаза и т. п.

Увеличившийся в последнее время интерес к данной тематике в мире принято связывать с угрозами активизировавшегося международного терроризма. Многие государства ввели в обращение паспорта с биометрическими данными.

• Вторая группа систем использует для идентификации динамические параметры: динамика воспроизведения подписи или рукописного ключевого слова, голос и т. п.

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 — самая распространенная, надежная и эффективная биометрическая технология. Благодаря универсальности этой технологии она может применяться практически в любой сфере и для решения любой задачи, где необходима достоверная идентификация пользователей. В основе метода лежит уникальность рисунка папиллярных узоров на пальцах. Отпечаток, полученный с помощью специального сканера, датчика или сенсора, преобразуется в цифровой код и сравнивается с ранее введенным эталоном. Надёжность данного способа идентификации личности состоит в невозможности создания идентичного отпечатка.

Наиболее совершенную технологию идентификации по отпечаткам пальцев реализуют оптические сканеры.

Характеристики идентификаторов

* Отпечатки всех пальцев каждого человека уникальны по рисунку папиллярных линий и различаются даже у близнецов. Отпечатки пальцев не меняются в течение всей жизни взрослого человека, они легко и просто предъявляются при идентификации.
* Если один из пальцев поврежден, для идентификации можно воспользоваться «резервным» отпечатком (отпечатками), сведения о которых, как правило, также вносятся в биометрическую систему при регистрации пользователя.

**Биометрические системы защиты информации**

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

Используемые в этих системах характеристики являются неотъемлемыми качествами личности человека и поэтому не могут быть утерянными и подделанными.

Обычно при классификации биометрических технологий выделяют две группы систем по типу используемых биометрических параметров:

• Первая группа систем использует статические биометрические параметры: отпечатки пальцев, геометрия руки, радужная оболочка глаза и т. п.

Увеличившийся в последнее время интерес к данной тематике в мире принято связывать с угрозами активизировавшегося международного терроризма. Многие государства ввели в обращение паспорта с биометрическими данными.

• Вторая группа систем использует для идентификации динамические параметры: динамика воспроизведения подписи или рукописного ключевого слова, голос и т. п.

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 радужной оболочке глаза:

Радужная оболочка глаза является уникальной для каждого человека биометрической характеристикой.

Радужная оболочка глаза человека не меняется в течение всей его жизни с самого рождения.

Ученые также провели ряд исследований, которые показали, что сетчатка глаза человека может меняться со временем, в то время как радужная оболочка глаза остается неизменной. И самое главное, что невозможно найти два абсолютно идентичных рисунка радужной оболочки глаза, даже у близнецов.

Система идентификации личности по радужной оболочке логически делится на две части: устройство захвата изображения, его первичной обработки и передачи вычислителю; вычислитель, производящий сравнение изображения с изображениями в базе данных, передающий команду о допуске исполнительному устройству

Для получения индивидуальной записи о радужной оболочке глаза черно-белая камера делает 30 записей в секунду. Еле различимый свет освещает радужную оболочку, и это позволяет видеокамере сфокусироваться на радужке. Одна из записей затем оцифровывается и сохраняется в базе данных зарегистрированных пользователей. Вся процедура занимает несколько секунд, и она может быть полностью компьютеризирована при помощи голосовых указаний и автофокусировки.

Очки и контактные линзы, даже цветные, никак не повлияют на процесс получения изображения. Также нужно отметить, что произведенные операции на глазах, удаление катаракты или вживление имплантатов роговицы не изменяют характеристики радужной оболочки, её невозможно изменить или модифицировать. Слепой человек также может быть идентифицирован при помощи радужной оболочки глаза. Пока у глаза есть радужная оболочка, её хозяина можно идентифицировать.

**Биометрические системы защиты информации**

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

Используемые в этих системах характеристики являются неотъемлемыми качествами личности человека и поэтому не могут быть утерянными и подделанными.

Обычно при классификации биометрических технологий выделяют две группы систем по типу используемых биометрических параметров:

• Первая группа систем использует статические биометрические параметры: отпечатки пальцев, геометрия руки, радужная оболочка глаза и т. п.

Увеличившийся в последнее время интерес к данной тематике в мире принято связывать с угрозами активизировавшегося международного терроризма. Многие государства ввели в обращение паспорта с биометрическими данными.

• Вторая группа систем использует для идентификации динамические параметры: динамика воспроизведения подписи или рукописного ключевого слова, голос и т. п.

Идентификация по характеристикам речи:

Голосовая биометрия, позволяющая измерять голос каждого человека, незаменима при удаленном обслуживании клиентов, когда основным средством взаимодействия является голос. Типы голосовой биометрии

Различаются 2 типа голосовой аутентификации:

1. Текстонезависимая - определение личности человека осуществляется по свободной речи, не требуется произнесения каких-то специальных слов и выражений. Например, человек может просто прочитать отрывок из стихотворения или обсудить с оператором контакт-центра цель своего звонка.

2. Текстозависимая - для определения личности человек должен произнести строго определенную фразу. При этом данный тип голосовой биометрии делится на два:

* + Текстозависимая аутентификация по статической парольной фразе - для проверки личности необходимо произнести ту же фразу, которая произносилась и при регистрации голоса данного человека в системе
  + Текстозависимая аутентификация по динамической парольной фразе - для проверки личности человека предлагается произнести фразу, состоящую из набора слов, произнесенных данным человеком при регистрации голоса в системе. Преимущество динамической парольной фразы от статической состоит в том, что каждый раз фраза меняется, что затрудняет мошенничество с использованием записи голоса человека (например, на диктофон).

не требуется специальных сканеров - достаточно обычного микрофона в телефоне или диктофоне, не предъявляется специальных требований к устройствам - может быть использован любой диктофон (аналоговый или цифровой), мобильный или стационарный телефон (хоть 80-х годов выпуска)

просто - не требуется специальных умений

Некоторые люди не могут произносить звуки;

голос может меняться в связи с заболеванием и с возрастом;

кроме того, на точность аутентификации влияет шумовая обстановка вокруг человека (шумы, реверберация).