

**Защита от  
несанкционированного  
доступа к информации  
11 класс**

**учитель информатики  
МБОУ «СОШ № 4»  
Сабельников А.А.**

**Наиболее острой проблемой современного общества является проблема информационной безопасности, начиная от отдельного человека до государства.**



**Защиту информации в компьютерах обязательно следует рассматривать как комплекс мер, включающих организационные, технические, юридические, программные, оперативные, страховые и даже морально-этические меры.**

**Не парадоксально ли, что воровство вещей из квартиры рассматривается как преступление, а воровство информации из компьютера зачастую как показатель высоких интеллектуальных возможностей?**

**И ни какой пароль, как, впрочем, и любая другая система безопасности, не поможет, если *каждый пользователь системы лично не заинтересован в соблюдении режима безопасности, не понимает, для чего нужен режим безопасности, и что этот пользователь лично потеряет в случае вскрытия его пароля или любого другого пароля в его организации. Ведь замок на двери можно открыть один раз утром и оставить открытым на весь день - какая же тогда безопасность?***

# Что же такое пароль?

Военные говорят:

**"пароль - это секретное слово, позволяющее определить кто 'свой', а кто нет".**

**С точки зрения компьютерной безопасности это определение можно немного добавить и расширить:**

**"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.**

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

# Пароли на компьютере

Информация о создании и изменении учетных записей, защищенных паролями, а также о доступе к ним и сведения о том, как установить защиту паролем при загрузке компьютера, находятся в файлах справки операционной системы или на веб-узле ее производителя. Например, в ОС Microsoft Windows XP информацию об управлении паролями, их изменении и т. д. можно найти в системе интерактивной справки.

**Храните пароль в надежном месте.  
Будьте внимательны, если  
записали пароль на бумажный или  
какой-либо другой носитель. Не  
оставляйте запись с паролем там,  
где бы вы не оставили  
информацию, которую он  
защищает.**

**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, если она составлена по всем правилам, приведенным выше.**

# Биометрические системы

## ЗАЩИТЫ

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

**Обилие биометрических методов поражает. Основными методами, использующими статистические биометрические характеристики человека, являются идентификация по папиллярному рисунку на пальцах, радужной оболочке, геометрии лица, сетчатке глаза человека, рисунку вен руки. Также существует ряд методов, использующих динамические характеристики человека: идентификация по голосу, динамике рукописного подчерка, сердечному ритму, походке.**

# Отпечатки пальцев

Дактилоскопия (распознавание отпечатков пальцев) — наиболее разработанный на сегодняшний день биометрический метод идентификации личности.

Катализатором развития метода послужило его широкое использование в криминалистике XX века.

Каждый человек имеет уникальный папиллярный узор отпечатков пальцев, благодаря чему и возможна идентификация. Обычно характерные точки на окончание линии узора — одиночные точки. Дополнительно информация о морфологии отпечатка пальца: от наличия замкнутых линий папиллярных спиральных линий. Основными преобразовываемыми в код сохраняются информация отпечатка. И именно «информация» хранятся в базе данных для сравнения. Время перекодирования пальца в код и его идентификация превышают 1с, в зависимости от сложности узора. Время, затраченное на идентификацию, учитывается.



зора

ка и  
атка

# Радужная оболочка

Радужная оболочка глаза является  
уникальной  
Рисунок ра  
восьмом м  
развития, о  
возрасте о  
изменяется  
результате  
патологий.  
наиболее т  
технологий

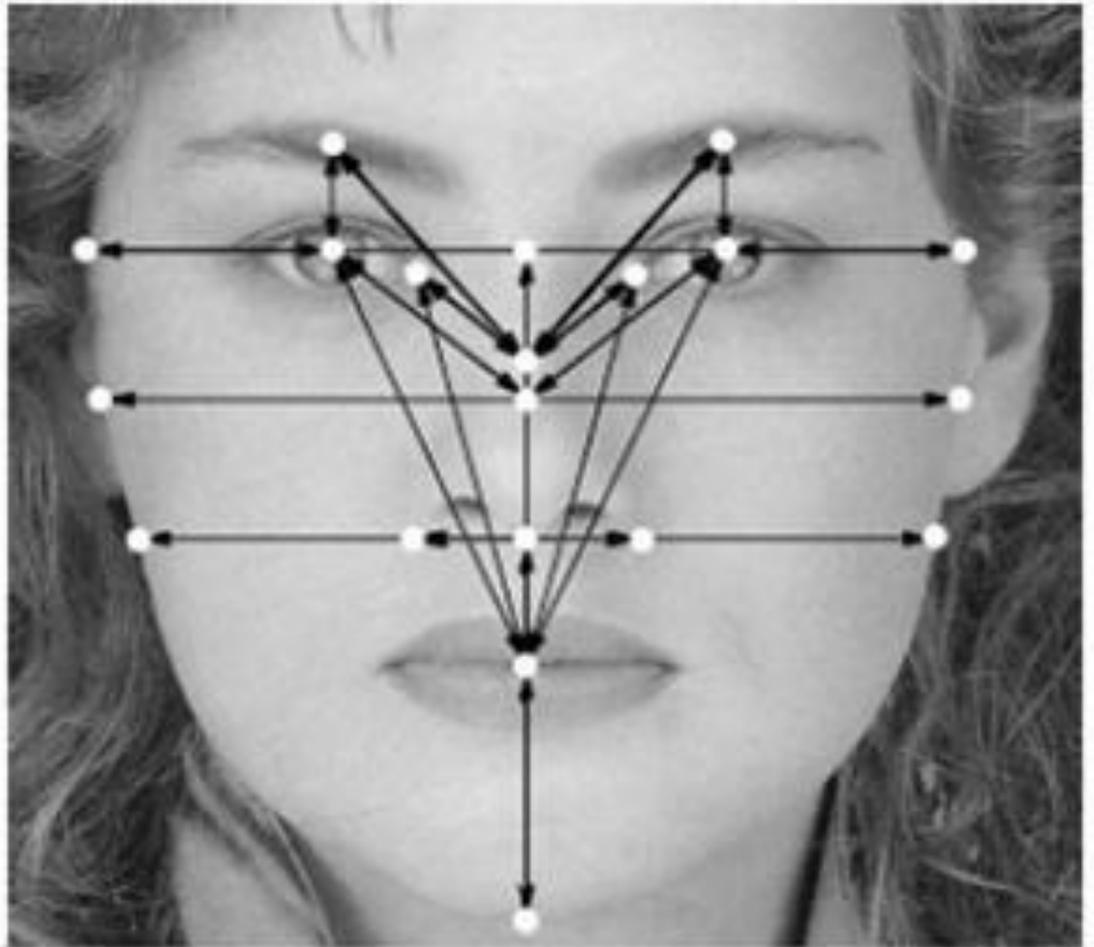


Система идентификации личности по радужной оболочке логически делится на две части: устройство захвата изображения, его первичной обработки и передачи вычислителю; вычислитель, производящий сравнение изображения с изображениями в базе данных, передающий команду о допуске исполнительному устройству.

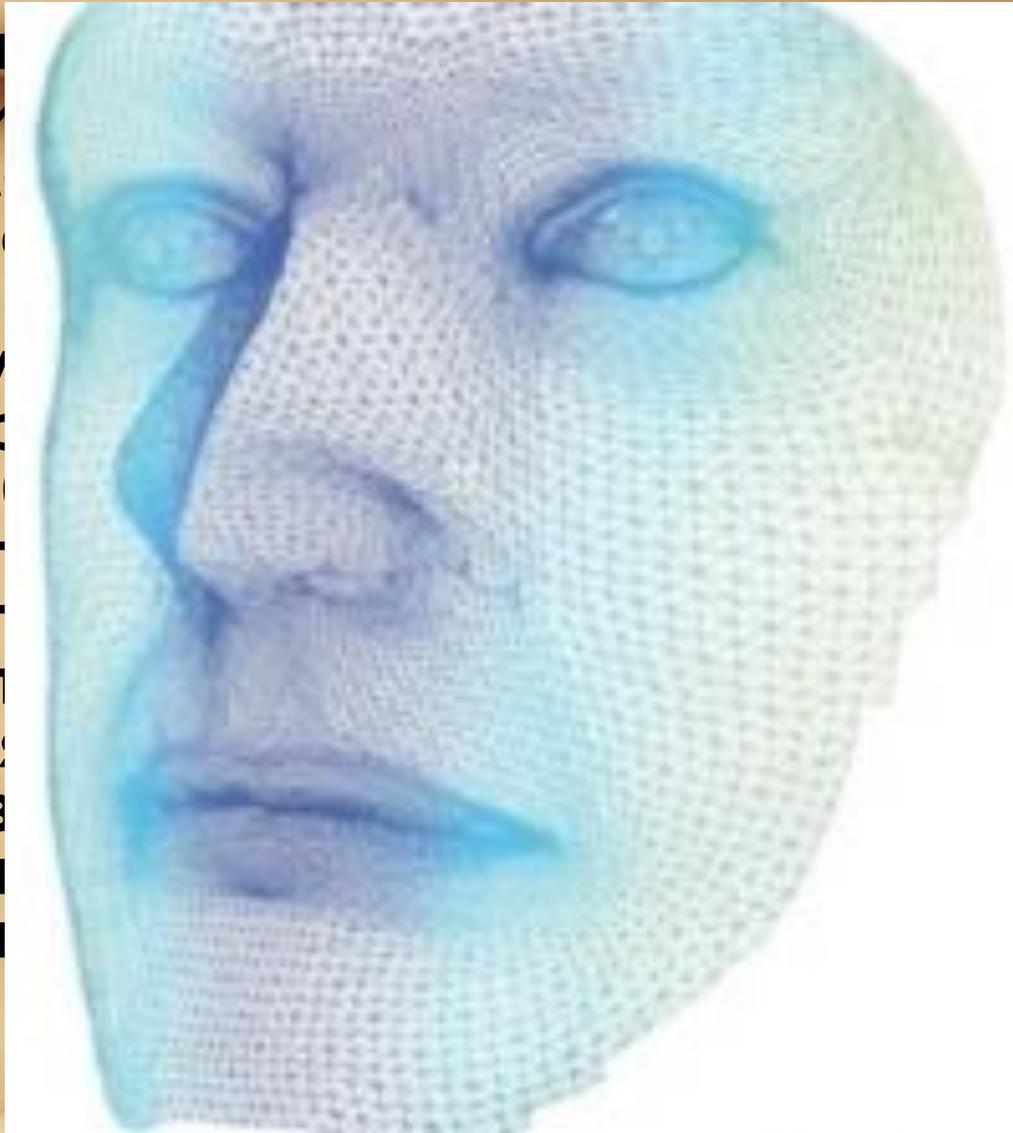
# Геометрия лица

Существует много методов по геометрии лица, так как черты лица человека индивидуальны. Биометрия многомерна, потому что мы можем измерять по лицу в два направления: для распознавания достоинства и качества, что зависит еще и от требований, предъявляемых к алгоритму.

2D-распознавание



2D-рас  
стати  
биом  
прим  
что и  
Впосл  
интер  
стал  
уступ  
уступ  
идент  
време  
показ  
мульт  
перен



ОСНОВНЫХ  
МЕТОДОВ  
ИЗДАВНО И  
СТАТИСТИКЕ,  
О.  
СОВРЕМЕННЫЕ  
МЕТОДЫ ЧЕГО ОН  
ИЗДАВНО,  
БОЛЬШЕ  
МЕТОДАМ  
ИЗДАВНО  
ОСНОВНОМ,  
ИЗДАВНО,

# Венозный рисунок руки

Это новая технология. Инфракрасная камера снимает внешнюю или внутреннюю вену. Рисунок вен формируется, потому что гемоглобин поглощает инфракрасное излучение. В результате на снимке видны черные линии. С помощью этой технологии на основе полученных данных создается цифровая свертка венозного рисунка человека со сканированием. Технология сравнительно проста, но имеет ряд минусов.



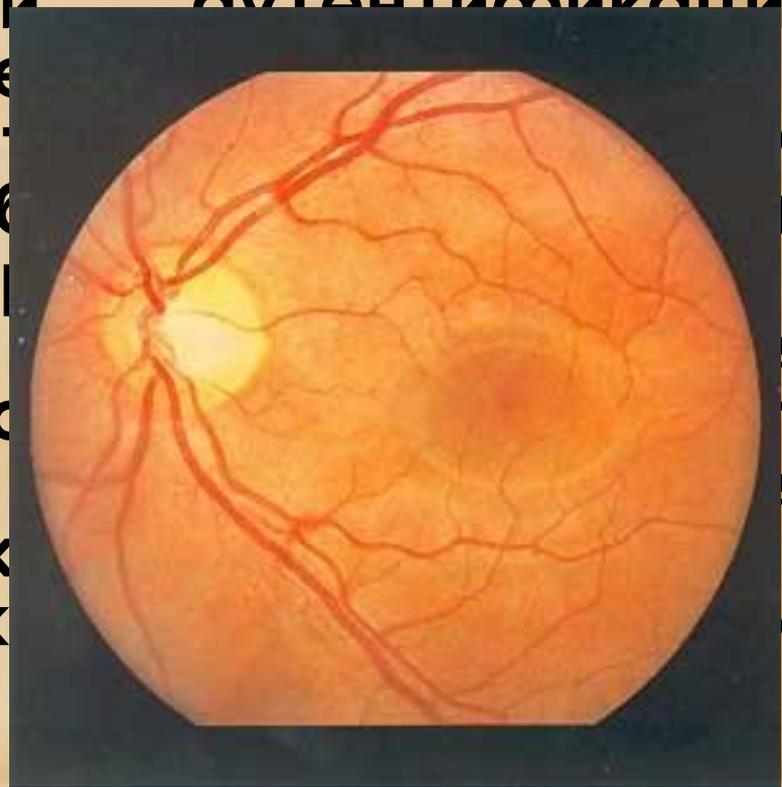
трии. Имиджи руки. Поэтому, ИК-излучения в виде а на вдает такта и с глаза,

# Преимущества и недостатки метода

Преимущества метода	Недостатки метода
<ul style="list-style-type: none"><li>• отсутствие необходимости контактировать со сканирующим устройством;</li><li>• высокая достоверность — статистические показатели метода сравнимы с показаниями радужной оболочки.</li></ul>	<ul style="list-style-type: none"><li>• недопустима засветка сканера солнечными лучами и лучами галогеновых ламп;</li><li>• некоторые возрастные заболевания, например артрит, сильно ухудшают FAR и FRR;</li><li>• метод менее изучен в сравнении с другими статическими методами биометрии.</li></ul>

# Сетчатка глаза

До последнего времени считалось, что самый надежный метод биометрической идентификации и аутентификации личности — это метод сканирования сетчатки. Сетчатка содержит в себе уникальные капилляры, которые используются для идентификации по рисунку капилляров по венам руки. рисунку капилляров сетчатки глаза. неподвижную структуру во времени, кроме как болезни, например,



**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.**

# Идентификация по голосу

Использует уникальные акустические особенности речи. Они отражают анатомию человека: размер и форма гортани и рта, а также приобретенные свойства громкость голоса, скорость и манера разговора. Идентификация по голосу заключается в том, что человека просят ответить на два-три вопроса, ответы на которые легко запомнить. Например: фамилия, имя, отчество; дата рождения. Некоторые современные системы создают модель голоса и могут сопоставлять ее с любой фразой, произнесенной человеком.

**Идентификация по подписи и другие поведенческие биометрические технологии основаны на измерении поведенческих характеристик человека. Это скорость письма, нажим и наклон букв, движение пера в момент подписи или написания текста. При идентификации по манере работы с клавиатурой снимаются такие показатели, как динамика нажатия на клавиши, ритм, манера пользователя нажимать на клавиши. К сожалению, несмотря на широкие области возможного применения, данные методики пока не получили достаточно широкого распространения.**

# Используемые материалы

- <http://>
- [http://passwords.lance.com.ua/article\\_protect\\_data\\_ru.htm](http://passwords.lance.com.ua/article_protect_data_ru.htm)[www.zahist.narod.ru/illusion.htm](http://www.zahist.narod.ru/illusion.htm)
- <http://www.zk-software.ru/>
- <http://www.polyset.ru/article/st327.php>
- [http://secandsafe.ru/stati/kompleksnye\\_sistem\\_y\\_bezopasnosti/biometricheckie\\_sistemy\\_identifikacii](http://secandsafe.ru/stati/kompleksnye_sistem_y_bezopasnosti/biometricheckie_sistemy_identifikacii)
- <http://smartcom.od.ua/safety-systems/biometric-system-identification>
- <http://habrahabr.ru/blogs/infosecurity/126144/>