Защита от несанкционированного доступа к информации

Немного истории:

В 1988 году американская Ассоциация компьютерного оборудования объявила ***30 ноября Международным днем защиты информации*** (Computer Security Day).

Целью Дня является напоминание пользователям о необходимости защиты их компьютеров и всей хранимой в них информации.

ЗАЩИЩАЕМАЯ ИНФОРМАЦИЯ

Защищаемая информация – это информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Собственником информации может быть - государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

ЦИФРОВАЯ ИНФОРМАЦИЯ

Цифровая информация – это информация, хранение, передача и обработка которой осуществляется средствами ИКТ.

2502 ЭБ
2012 г

468 ЭБ
2008 г

Результаты исследования International Data Corporation (IDC) , 2008 год

ЗАЩИТА ИНФОРМАЦИИ

Защита информации - деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Несанкционированное воздействие – это преднамеренная порча или уничтожение информации со стороны лиц не имеющих на это права.

Непреднамеренное воздействие происходит вследствие ошибок пользователя, а также из-за сбоев оборудования или программного обеспечения.

ВИДЫ УГРОЗ

Угроза утечки	
Преднамеренная кража, копирование	
Проникновение в память компьютера, в базы данных информационных систем.	Перехват в каналах передачи данных, искажение, подлог данных.

Цифровые носители для хранения данных – объекты краж.

Новый канал утечки – кража через сети.

ВИДЫ УГРОЗ

Угроза разрушения	
Несанкционированное разрушение	**Непреднамеренное разрушение**
Вредоносные программные коды - вирусы; деятельность хакеров, атаки.	Ошибки пользователя, сбои оборудования, ошибки и сбои в работе ПО, форс-мажорные обстоятельства.

Хакеры – «взломщики» информационных систем с целью воздействия на их содержание и работоспособность.

Атака – это одновременное обращение с большого количества компьютеров на сервер информационной системы.

СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ

- ✓ Физическая защита каналов
- ✓ Использование источников бесперебойного питания
- ✓ Контроль и профилактика оборудования
- ✓ Резервное копирование информации
- ✓ Использование надежных паролей
- ✓ Разграничение доступа
- ✓ Брандмауэры
- ✓ Межсетевые экраны
- ✓ Антивирусные программы

АНТИВИРУСНЫЕ ПРОГРАММЫ

- Антивирусы лаборатории Касперского
- Dr .Web
- ESET NOD32
- AVAST
- McAfee Antivirus
- Symantec

ЦИФРОВАЯ ПОДПИСЬ

Цифровая подпись - это индивидуальный секретный шифр, ключ которого известен только владельцу.

Цифровая подпись предназначена для защиты электронного документа и является результатом криптографического преобразования информации с использованием закрытого ключа .

Закрытый ключ – это ключ, которым заранее обмениваются два абонента, ведущие секретную переписку.

ЦИФРОВОЙ СЕРТИФИКАТ

Цифровой сертификат - это сообщение, подписанное полномочным органом сертификации, который подтверждает, что открытый ключ действительно относится к владельцу подписи.

Открытый ключ передается с документом заверенным цифровой подписью для ее расшифровки.

Один из применяемых элементов защиты - пароль (а в некоторых он единственный), который многие пользователи и руководители считают непреодолимым препятствием.

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.

Какие правила можно рекомендовать при выборе пароля?

Запрещается использовать:

- имена, фамилии, даты рождения детей, близких, знакомых, их ком-бинации, номера телефонов и любую другую личную информацию (типа ОЛЯ070576 или ИВАНОРЛОВ) и т.п.;
- названия городов, стран, фирм, организаций, учреждений, специфических компьютерных слов, термины из своей предметной области;
- слова из заставок задач или названия самих компьютерных систем (например, netware, windows, msdos);
- широко распространенные слова, названия фильмов, книг, имена любимых литературных героев и пр.;
- повторяющиеся символы (например, пароль типа "аббббб" раскрыть значительно легче, чем "алугыс");
- набор символов, расположенных на клавиатуре рядом (“знаменитые” пароли: 111111, 12345, йцукен, qwerty и т.д.) или по простому закону (например, через клавишу - йу-егщх; по две в ряду - йцфыяч и т.п.);
- нельзя использовать один и тот же пароль одновременно в разных системах. Это прекрасная возможность для хакера проникнуть в систему.

Рекомендуется использовать:

- Переключения различных регистров (рус., англ.). Попробуйте набрать русское слово на английском регистре или наоборот, получите бессмысленный набор, вполне подходящий для пароля. Можно, например, взять слово из любого (желательно не английского) языка и его звучание на русском языке набрать на английском регистре.
- Использовать при формировании пароля как можно большее количество символов, конечно, если это допускает система (ведь компьютер позволяет использовать 256 символов). Например, сочетания букв и цифр, а также больших и маленьких букв в одном пароле (например, "ащночс" и "АщНоЧс" для компьютера - две большие разницы) значительно усложняет его подбор;
- Если с фантазией «напряженка» попробуйте просто связать два слова вместе, например: «ЯГений», «МояЖенаУмница», «ЛюблюВасю»

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.

Хранение паролей в секрете

Относитесь к паролям и идентификационным фразам так же серьезно, как к информации, которую они защищают.

Никому не сообщайте пароль. Держите пароль в секрете от своих близких (особенно от детей) и друзей, которые могут сообщить его кому-либо еще. Исключением являются пароли, которые необходимо знать вашим близким.

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.

Никогда не пересылайте пароль по электронной почте. Любое сообщение электронной почты, требующее ваш пароль или отсылающее на веб-узел для подтверждения пароля, может быть мошенничеством.

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.

Не вводите пароли на чужих компьютерах. Компьютеры в интернет-кафе, лабораториях, системах с коллективными файлами, интерактивных терминалах, на конференциях безопасны только для анонимного выхода в Интернет. Не пользуйтесь такими компьютерами для проверки электронной почты, банковского счета, доступа в чат-каналы и доступа к другим учетным записям, где запрашивается имя пользователя и пароль.

Биометрические системы защиты

Современные биометрические методы идентификации

12.12.2022

Технология биометрической идентификации уже заняла прочные позиции на рынке систем безопасности благодаря ее основному достоинству — производится идентификация физиологических особенностей человека, а не ключа или карточки.

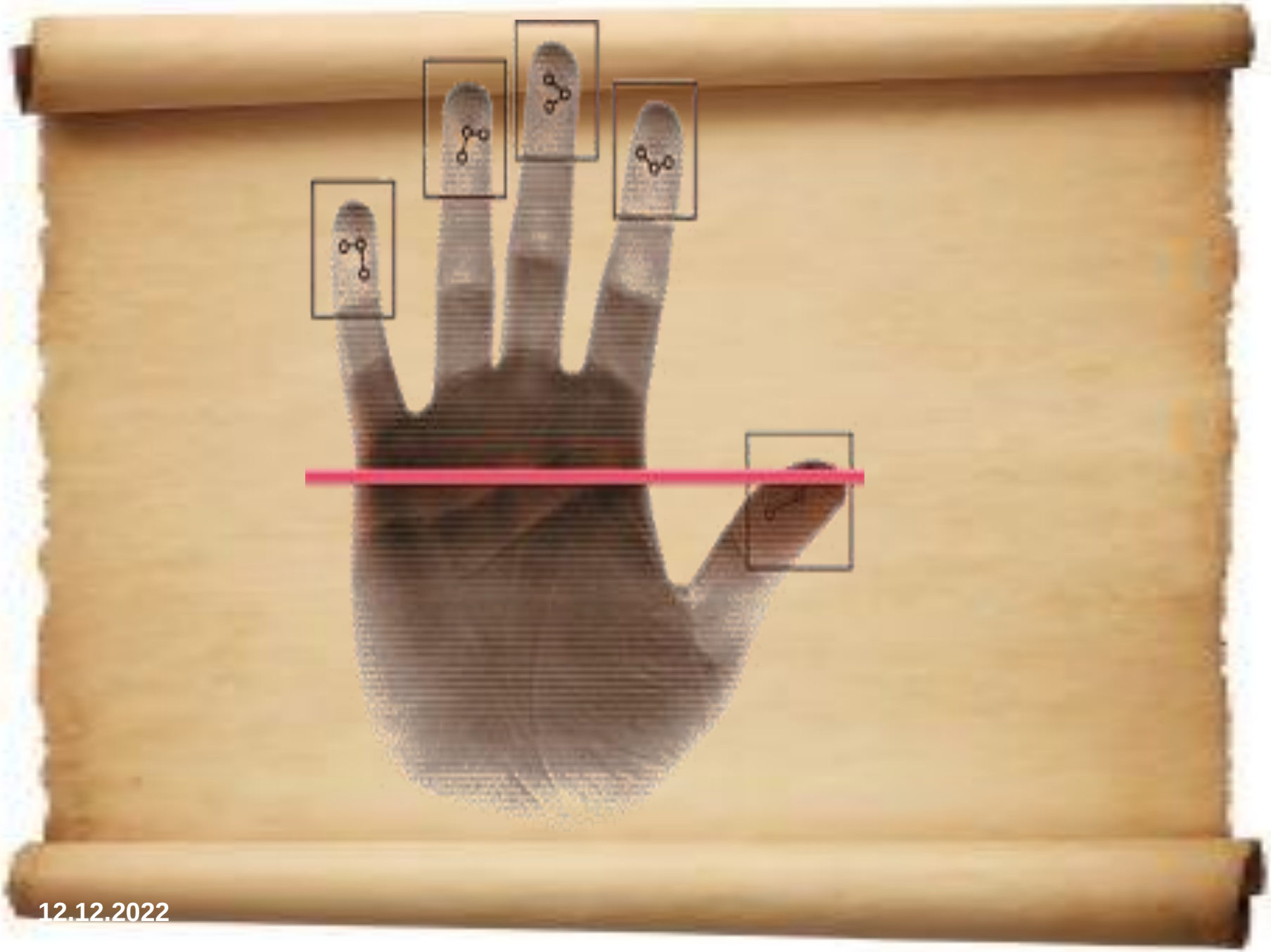
Биометрическая идентификация **- это способ идентификации личности по отдельным специфическим биометрическим признакам (идентификаторам), присущим конкретному человеку**

За последние два десятилетия биометрические технологии сделали большой шаг вперед. Во многом этому способствовало распространение микропроцессорных технологий. Еще в 80-е годы систему контроля доступа, использующую биометрические характеристики человека, можно было увидеть лишь в фантастических фильмах. Сегодня же использование в системах контроля и управления доступом (СКУД) биометрических сканеров, практически, не усложняет систему безопасности, и их стоимость для некоторых биометрических методов очень низкая. Более того, около трети ноутбуков выходит сейчас со встроенной системой считывания отпечатка пальцев, а если в ноутбуке есть видеокамера, на него можно установить систему распознавания человека по лицу.

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.



12.12.2022

Каждый человек имеет уникальный папиллярный узор отпечатков пальцев, благодаря чему и возможна идентификация. Обычно алгоритмы используют характерные точки на отпечатках пальцев: окончание линии узора, разветвление линии, одиночные точки. Дополнительно привлекается информация о морфологической структуре отпечатка пальца: относительное положение замкнутых линий папиллярного узора, арочных и спиральных линий. Особенности папиллярного узора преобразовываются в уникальный код, который сохраняет информативность изображения отпечатка. И именно «коды отпечатков пальцев» хранятся в базе данных, используемой для поиска и сравнения. Время перевода изображения отпечатка пальца в код и его идентификация обычно не превышают 1с, в зависимости от размера базы. Время, затраченное на поднесение руки, не учитывается.


Welcome Check-In
05:27
05-08-10 WEC
1 2 3 ESC
4 5 6 ▲ IN
7 8 9 ▼OUT
0 OK MENU
F4 Vista
Access control

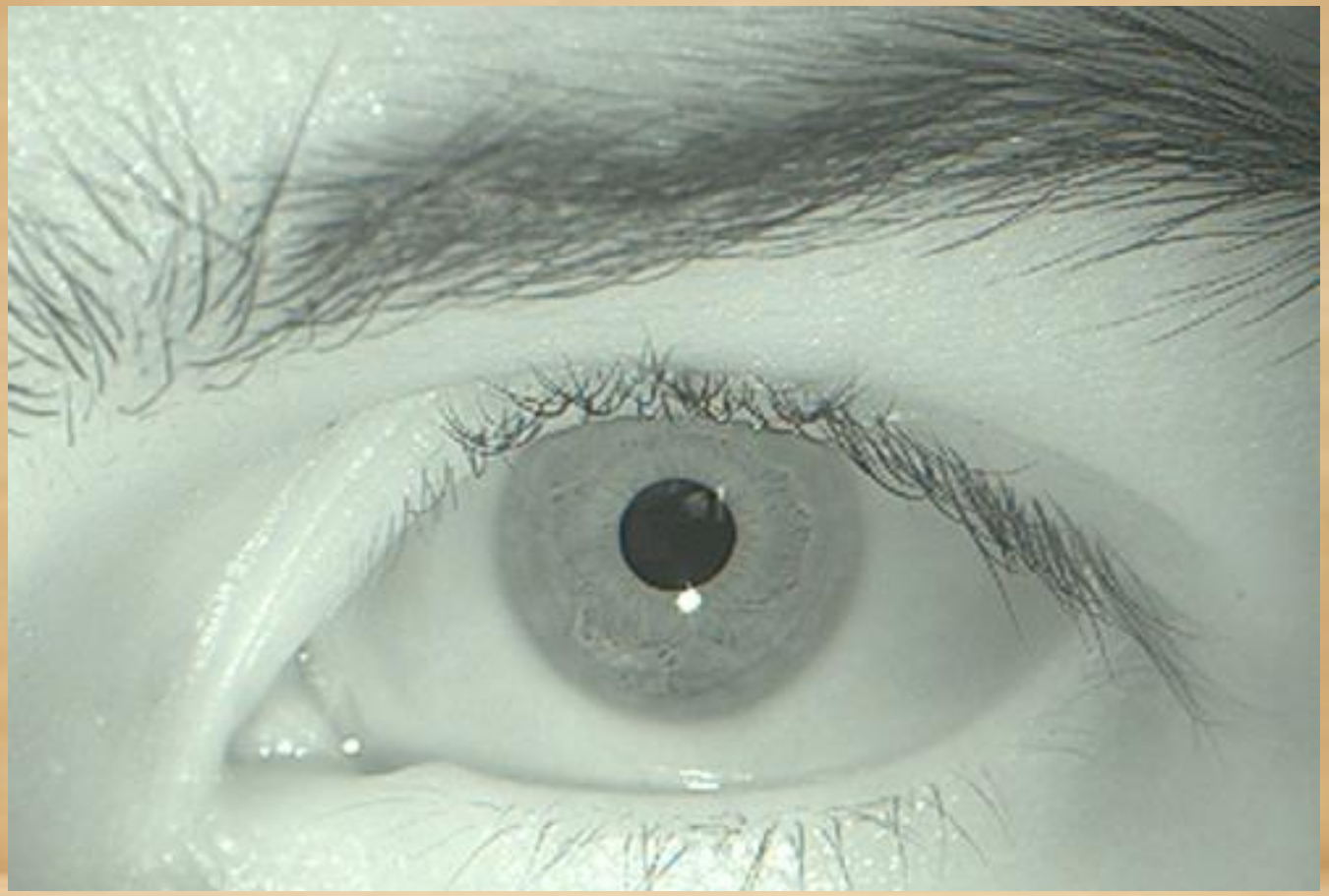
12.12.2022

Преимущества и недостатки метода:

Преимущества метода	Недостатки метода
• высокая достоверность — статистические показатели метода выше показателей способов идентификации по лицу, голосу, росписи; • низкая стоимость устройств, сканирующих изображение отпечатка пальца; • достаточно простая процедура сканирования отпечатка.	• папиллярный узор отпечатка пальца очень легко повреждается мелкими царапинами, порезами; • недостаточная защищенность от подделки изображения отпечатка, отчасти вызванная широким распространением метода.

Радужная оболочка

Радужная оболочка глаза является уникальной характеристикой человека. Рисунок радужки формируется на восьмом месяце внутриутробного развития, окончательно стабилизируется в возрасте около двух лет и практически не изменяется в течение жизни, кроме как в результате сильных травм или резких патологий. Метод является одним из наиболее точных среди биометрических технологий.



12.12.2022

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.

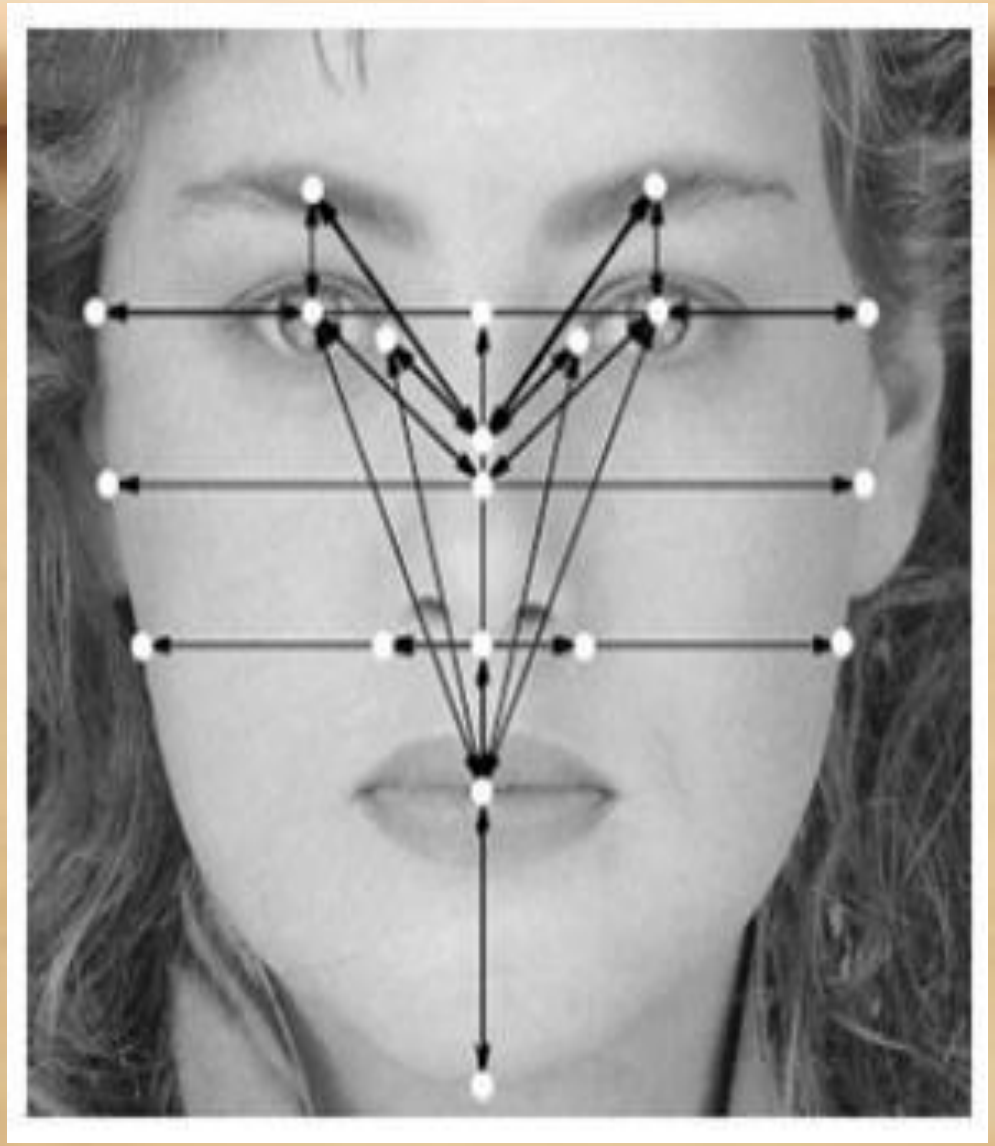
Преимущества и недостатки метода:

Преимущества метода	Недостатки метода
• статистическая надежность метода; • захват изображения радужной оболочки можно производить на расстоянии от нескольких сантиметров до нескольких метров, при этом физический контакт человека с устройством не происходит; • радужная оболочка защищена от повреждений роговицей (например, отпечатки пальцев легко портятся царапинами или пачкаются); • большое количество методов противодействия подделкам.	• цена системы для захвата радужной оболочки выше стоимости сканера отпечатка пальца и камеры для захвата 2D изображения лица.

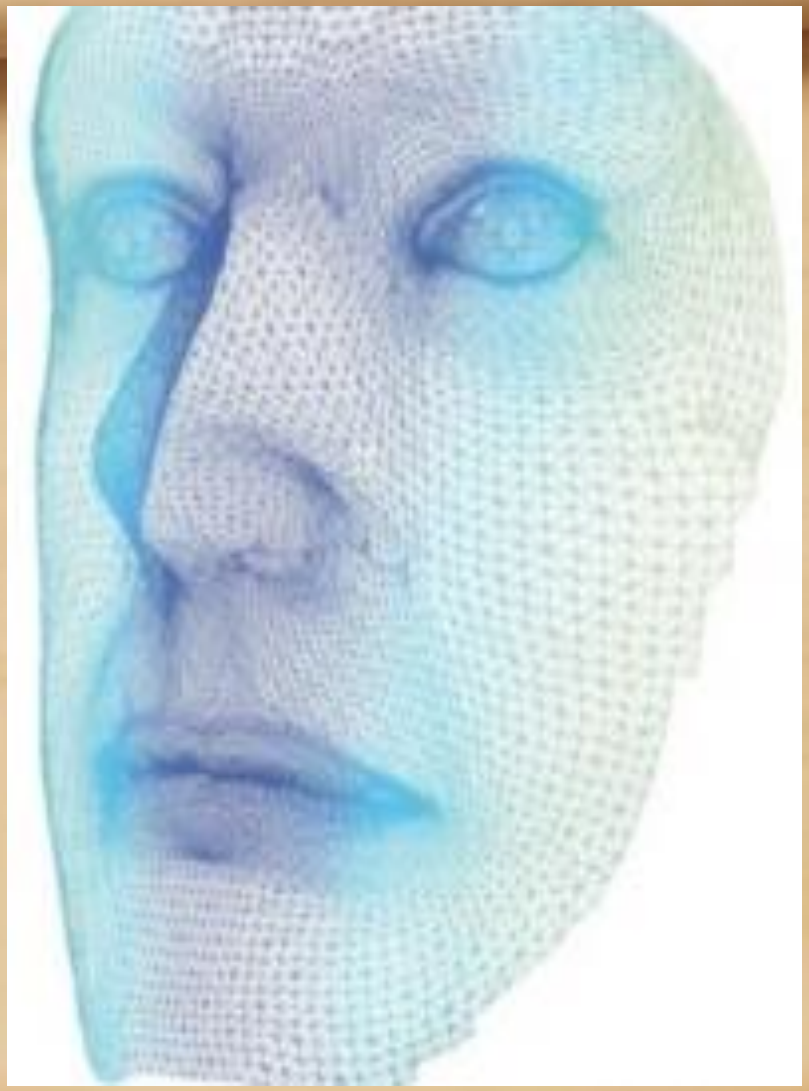
Геометрия лица

Существует множество методов распознавания по геометрии лица. Все они основаны на том, что черты лица и форма черепа каждого человека индивидуальны. Эта область биометрии многим кажется привлекательной, потому что мы узнаем друг друга в первую очередь по лицу. Данная область делится на два направления: 2D-распознавание и 3D-распознавание. У каждого из них есть достоинства и недостатки, однако многое зависит еще и от области применения и требований, предъявленных к конкретному алгоритму.

2D-распознавание лица



2D-распознавание лица — один из самых статистически неэффективных методов биометрии. Появился он довольно давно и применялся, в основном, в криминалистике, что и способствовало его развитию. Впоследствии появились компьютерные интерпретации метода, в результате чего он стал более надежным, но, безусловно, уступал и с каждым годом все больше уступает другим биометрическим методам идентификации личности. В настоящее время из-за плохих статистических показателей он применяется, в основном, в мультимодальной или, как ее еще называют, перекрестной биометрии.



12.12.2022

Преимущества и недостатки метода

Преимущества метода	Недостатки метода
• при 2D-распознавании, в отличие от большинства биометрических методов, не требуется дорогостоящее оборудование; • возможность распознавания на значительных расстояниях от камеры.	• низкая статистическая достоверность; • предъявляются требования к освещению (например, не удается регистрировать лица входящих с улицы людей в солнечный день); • для многих алгоритмов неприемлемость каких-либо внешних помех, как, например, очки, борода, некоторые элементы прически; • обязательно фронтальное изображение лица, с весьма небольшими отклонениями; • многие алгоритмы не учитывают возможные изменения мимики лица, т.е. выражение должно быть нейтральным.

Венозный рисунок руки

Это новая технология в сфере биометрии. Инфракрасная камера делает снимки внешней или внутренней стороны руки. Рисунок вен формируется благодаря тому, что гемоглобин крови поглощает ИК-излучение. В результате степень отражения уменьшается и вены видны на камере в виде черных линий. Специальная программа на основе полученных данных создает цифровую свертку. Не требуется контакта человека со сканирующим устройством.

Технология сравнима по надежности с распознаванием по радужной оболочке глаза, но имеет ряд минусов, указанных ниже.

12.12.2022

Преимущества и недостатки метода

Преимущества метода	Недостатки метода
• отсутствие необходимости контактировать со сканирующим устройством; • высокая достоверность — статистические показатели метода сравнимы с показаниями радужной оболочки.	• недопустима засветка сканера солнечными лучами и лучами галогеновых ламп; • некоторые возрастные заболевания, например артрит, сильно ухудшают FAR и FRR; • метод менее изучен в сравнении с другими статическими методами биометрии.

Сетчатка глаза

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.

Преимущества и недостатки метода:

Преимущества метода	Недостатки метода
• высокий уровень статистической надежности; • из-за низкой распространенности систем мала вероятность разработки способа их «обмана»; • бесконтактный метод снятия данных.	• сложная при использовании система с долгим временем обработки; • высокая стоимость системы; • отсутствие широкого рынка предложения и, как следствие, недостаточная интенсивность развития метода.

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.

Существуют различные прогнозы по развитию биометрического рынка в будущем, однако в целом можно сказать о сохранении тенденции к его дальнейшему росту. Что же касается отдельных сегментов биометрического рынка, здесь эксперты в основном сходятся во мнениях. Так, идентификации по отпечаткам пальцев они отводят в ближайшие годы все еще более половины рынка. Далее следует распознавание по геометрии лица и радужной оболочке. Это так называемые «три большие биометрики». За ними идут остальные методы распознавания примерно в такой последовательности: геометрия руки, рисунок вен, голос, подпись.

Российское законодательство в области информационной безопасности

Уровни мер по защите интересов субъектов информационных отношений

- законодательный;
- административный (приказы и другие действия руководства организаций, связанных с защищаемыми информационными системами);
- процедурный (меры безопасности, ориентированные на людей);
- программно-технический.

Группы мер на законодательном уровне

- меры, направленные на создание и поддержание в обществе негативного (в том числе с применением наказаний) отношения к нарушениям и нарушителям информационной безопасности (назовем их *мерами ограничительной направленности*);
- *направляющие и координирующие меры,* способствующие повышению образованности общества в области информационной безопасности, помогающие в разработке и распространении средств обеспечения информационной безопасности (меры созидательной направленности).

Основным законом Российской Федерации является Конституция, принятая 12 декабря 1993 года.

- **В соответствии со статьей 24 Конституции, органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.**
- **Статья 41 гарантирует право на знание фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, статья 42 - право на знание достоверной информации о состоянии окружающей среды.**
- **В принципе, *право на информацию* может реализовываться средствами бумажных технологий, но в современных условиях наиболее практичным и удобным для граждан является создание соответствующими законодательными, исполнительными и судебными органами информационных серверов и поддержание доступности и целостности представленных на них сведений, то есть обеспечение их (серверов) информационной безопасности.**
- **Статья 23 Конституции гарантирует *право на личную и семейную тайну*, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, статья 29 - право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Современная интерпретация этих положений включает обеспечение конфиденциальности данных, в том числе в процессе их передачи по компьютерным сетям, а также доступ к *средствам защиты информации*.**

Гражданский кодекс Российской Федерации

- **Согласно статье 139, информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности. Это подразумевает, как минимум, компетентность в вопросах ИБ и наличие доступных (и законных) средств обеспечения конфиденциальности.**

Уголовный кодекс Российской Федерации (редакция от 11 января 2018 года).

- Глава 28 - "Преступления в сфере компьютерной информации" - содержит три статьи:
- статья 272. Неправомерный доступ к компьютерной информации;
- статья 273. Создание, использование и распространение вредоносных программ для ЭВМ;
- статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.
- Первая имеет дело с посягательствами на конфиденциальность, вторая - с вредоносным ПО, третья - с нарушениями доступности и целостности, повлекшими за собой уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ. Включение в сферу действия УК РФ вопросов доступности информационных сервисов представляется нам очень своевременным.
- Статья 138 УК РФ, защищая конфиденциальность персональных данных, предусматривает наказание за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений. Аналогичную роль для банковской и коммерческой тайны играет статья 183 УК РФ.

Закон от 21 июля 1993 г. №5485-I "О государственной тайне» (последняя редакция 26 июля 2017 г.)

- **В нем гостайна определена как защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Там же дается определение средств защиты информации. Согласно данному Закону, это технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих *государственную тайну*; средства, в которых они реализованы, а также средства контроля эффективности защиты информации. Подч важность последней части определения.**

Закон № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации» (последняя редакция 1 января 2018 года)

- **В нем даются основные определения, намечаются направления, в которых должно развиваться законодательство в данной области, регулируются отношения, возникающие при:**
- **осуществлении права на поиск, получение, передачу, производство и распространение информации;**
- **применении информационных технологий;**
- **обеспечении защиты информации.**

Основные определения

- **информация** - сведения (сообщения, данные) независимо от формы их представления;
- **информационные технологии** - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
- **информационная система** - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
- **информационно-телекоммуникационная сеть** - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;
- **обладатель информации** - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;
- **доступ к информации** - возможность получения информации и ее использования;
- **конфиденциальность информации** - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;
- **предоставление информации** - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

- **распространение информации** - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;
- **электронное сообщение** - информация, переданная или полученная пользователем информационно-телекоммуникационной сети;
- **документированная информация** - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;
- **оператор информационной системы** - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации:

- свобода поиска, получения, передачи, производства и распространения информации любым законным способом;
- установление ограничений доступа к информации только федеральными законами;
- открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;
- равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;
- обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;
- достоверность информации и своевременность ее предоставления;
- неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;
- недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Другие законы и нормативные акты

- Закон "О лицензировании отдельных видов деятельности" от 8 августа 2001 года № 128-ФЗ
- Закон "Об участии в международном информационном обмене" от 4 июля 1996 года № 85-ФЗ
- Закон "Об электронной цифровой подписи" № 1-ФЗ
- Федеральный закон "О Персональных данных" от 27 июля 2006 года № 152-ФЗ

Спасибо за внимание