Санкт-Петербургский государственный университет информационных технологий, механики и оптики

Описание практической работы студентов (ЛП) по дисциплине «Системы представления знаний»

Новиков Ф.А.,
к.ф.-м.н., доцент кафедры «Технологии программирования»

Санкт-Петербург
2007

Оглавление

Цель проведения семинаров

Лабораторный практикум по курсу «Системы представления знаний» выполняется в форме семинаров с докладами студентов. Каждый студент в течение семестра должен подготовить и провести один семинар на выбранную тему.

Целью лабораторного практикума по дисциплине «Системы представления знаний» является:

- изучение студентом новейших достижений искусственного интеллекта в отдельной выбранной предметной области;
- приобретение практических навыков подготовки презентаций и демонстраций с помощью компьютера;
- приобретение опыта владения аудиторией при проведении презентации.

Список тем семинаров для выбора

1. Экспертные системы
2. Функциональное программирование
3. Фреймы и семантические сети
4. Управление роботами
5. Синтез речи
6. Семантические сети и фреймы
7. Распознавание текста
8. Распознавание речи
9. Распознавание образов человека
10. Программирование интеллектуальных игр
11. Поиск путей в синтетических 3D-пространствах
12. Нормальные алгорифмы и язык Refal
13. Нечеткие множества и нечеткие рассуждения
14. Механизмы работы памяти человека
15. Машинный перевод
16. Машинное зрение: распознавание трёхмерных сцен
17. Лямбда-исчисление и язык Lisp
18. Логическое программирование и язык Prolog
19. Искусственные нейронные сети
20. Извлечение знаний из баз данных: data mining
21. Генетические алгоритмы
22. Автоматное программирование
23. Автоматическое тестирование программ и model checking
24. Автоматическое доказательство теорем
25. Автоматический синтез программ

Требования к подготовке и проведению семинара

Основываясь на рекомендуемых учебных материалах и путем анализа выбранной предметной области, изучая различные источники, в том числе

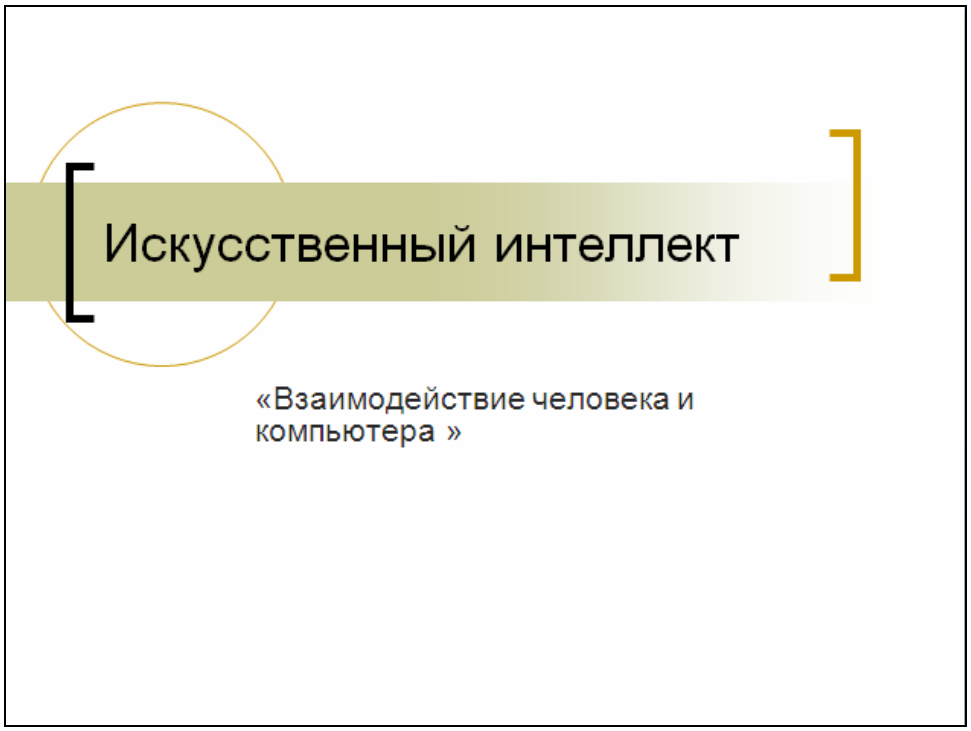
- лекционный материал;
- материалы семинаров прежних лет;
- Интернет

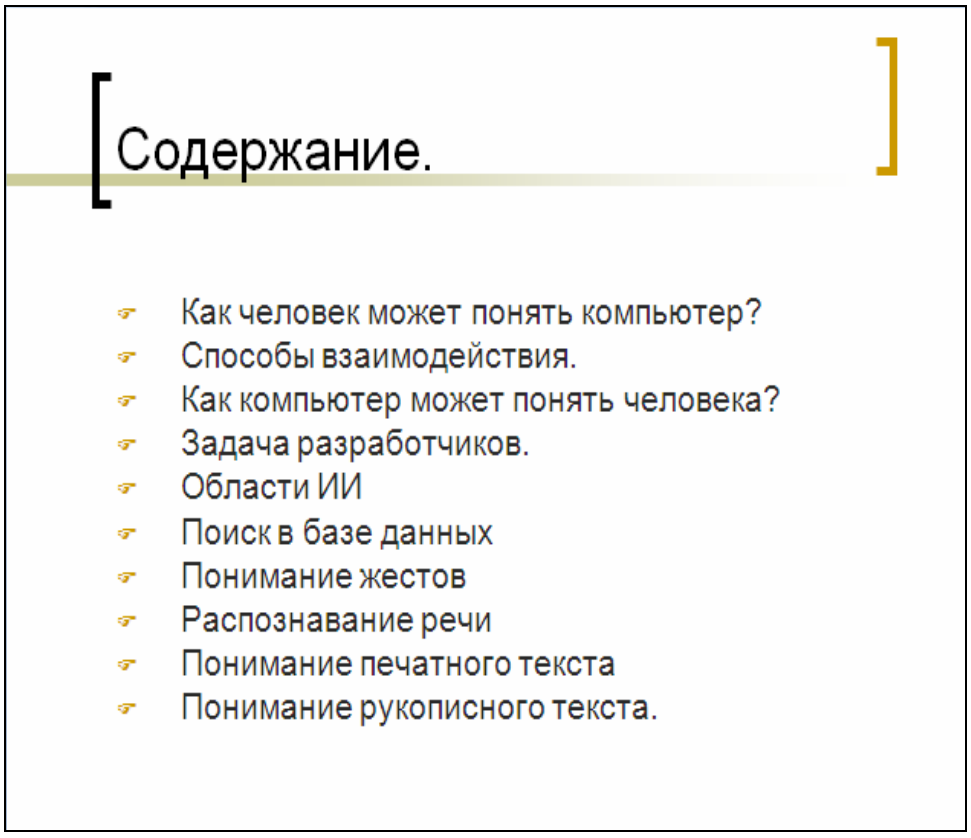
каждый студент должен подготовить семинар, отвечающий следующим требованиям:

- семинар должен включать доклад на выбранную тему продолжительностью не менее 1 академического часа;
- для наглядности изложения материала, последний должен быть представлен в форме презентации MS Power point;
- презентация должна содержать не менее 30 слайдов;
- необходимо указывать все источники, использованные при подготовке к семинару;
- допускаются демонстрации программ.

После доклада происходит обсуждение изложенного материала в форме ответов докладчика на вопросы слушающих.

Приложение 1. Пример презентации на тему «Взаимодействие человека и компьютера»





Как человек может понять компьютер?

5DT Data Glove 5

информационная перчатка
(устройство ввода данных
в системах виртуальной реальности,
воспринимающая движение руки
пользователя и передающее
их в компьютер)

Современный волоконно-оптический гибкий сенсор генерирует данные изгиба пальцев (по 1 сенсору на каждый палец). Воспринимает движения руки, угол наклона и вращение. Может использоваться вместо мышки или джойстика. Связь с компьютером через кабель или беспроводная через радио связь на расстоянии до 20 м.

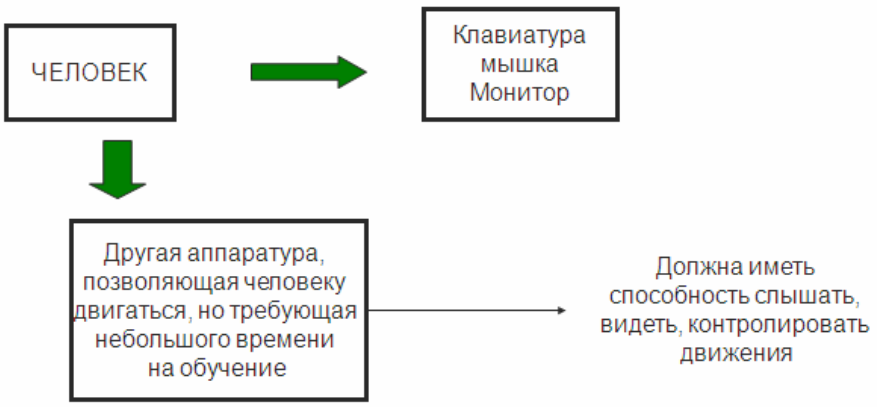
Fifth Dimension Technologies

Способы взаимодействия:

- Слух – уши, тело - **sound**
- Зрение – глаза - **image**
- Осязание – кожа - **surface / temperature**
- Обоняние – нос - **odour**
- Вкус – язык/нос - **savour, flavour**

Все чувства могут быть переведены в числа, но не все нужны для приложений.

Как компьютер может понять человека?



Задача разработчиков:

создать интерактивный, интуитивно понятный интерфейс, разработанный при помощи технологий, использующих знания из лингвистики, искусственного интеллекта и обучения на опыте.

Области ИИ,

которые исследуется и имеет широкое применение в настоящее время:

- Понимание ЕЯ (поиск в БД, поиск в Internet)
- Понимание ЕЯ (печатный текст)
- Понимание ЕЯ (рукописный текст)
- Распознавание речи
- Распознавание движения и жестов

Виртуальная реальность использует max возможностей ИИ, т.к. пытается воспроизвести мир и человека.

Поиск в базе данных

- Центр тяжести исследований в этой области пришелся на английский, т.к. законы его строения (грамматика) исследованы вдоль и поперек.
- Рассмотрим пример естественно-языкового (ЕЯ) интерфейса к базам данных - каталогами товаров. Эта область находит наибольшее применение. Ну что бы не спросить на каком-нибудь сайте: «найди мне цифровой фотоаппарат о трех мегапикселах, да подешевле»?
- Вопрос человеку понятен, любой консультант-продавец в магазине, если он владеет русским языком, знает, что такое цифровой фотоаппарат, и хоть немного представляет себе его основные свойства, вопрос поймет и худо-бедно на него ответит. Если изучить механизм понимания этого вопроса и других подобных, то можно создать понимающую систему. По аналогии. Главное здесь - уяснить, как человек понимает вопросы

Морфологический разбор запроса.

- ***Найди*** - глагол в повелительном наклонении;
- ***мне*** - личное местоимение 1-го лица в дательном падеже;
- ***цифровой*** - прилагательное мужского рода, единственного числа, в винительном падеже;
- ***фотоаппарат*** - существительное мужского рода, единственного числа, в винительном падеже;
- ***о*** - предлог;
- ***трех*** – числительное;
- ***мегапикселах*** - существительное мужского рода, единственного числа, в предложном падеже;
- ***да*** - союз;
- ***подешевле*** - прилагательное в сравнительной форме.

Синтаксический разбор

- найди (что сделай?) - сказуемое;
- мне (кому?) - косвенное дополнение;
- цифровой фотоаппарат (что?) - прямое дополнение;
- о трех мегапикселах (какой?) - определение;
- да подешевле (какой?) - определение.

Семантический анализ

Показывает на вольность языка автора. Оборот «о 3 мегапикселях» поставит систему в тупик. Предположим, система все-таки знает о такой вольности, как употребление предложного падежа там, где должен быть творительный с соответствующим предлогом (с кем, чем?). найди (кому) мне (какой, характеристика) цифровой (что, объект) фотоаппарат (какой, характеристика) о трех мегапикселах (какой, характеристика) подешевле.

Прагматика.

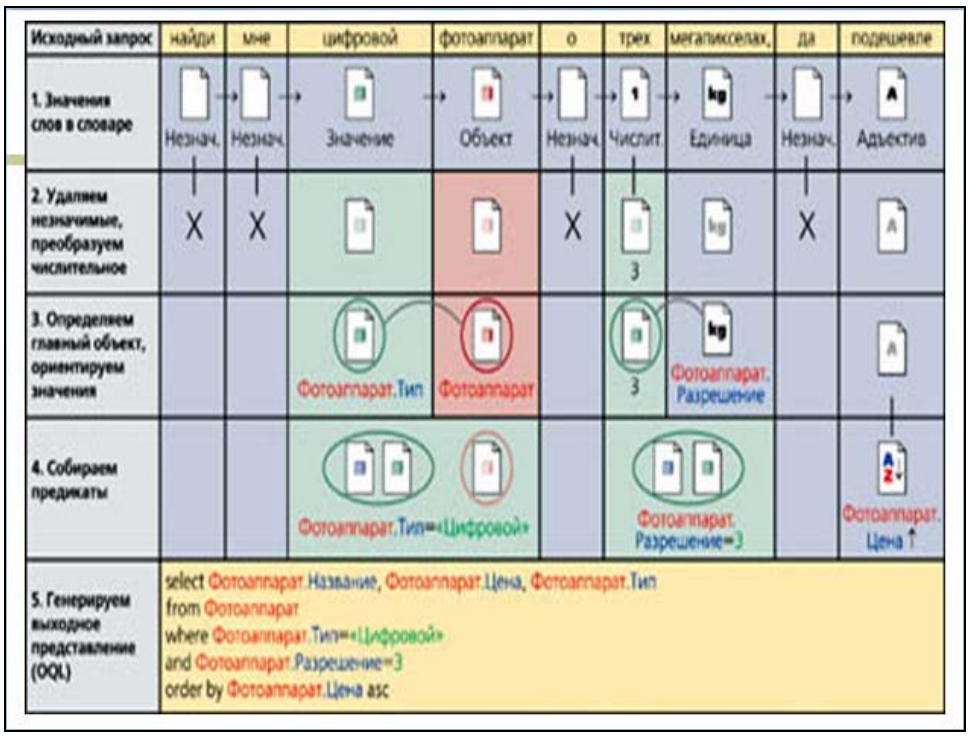
Переводим запрос на формальный язык:

- найди X Команда = искать;
- цифровой X Тип = цифровой;
- фотоаппарат X КлассОбъекта = фотоаппарат;
- трех мегапикселах X Разрешение = 3;
- подешевле X цена (низкая).

Вывод.

Первоначальные знания (морфология, синтаксис) перешли через семантику в прагматику, а знания о языке - в знания о предметной области.

Многие знания оказались здесь лишними! Иллюстрация – в таблице:



Проблемы:

Проблема понимания запросов к каталогу товаров уже решена, однако проблема понимания машиной естественного языка вообще - поглотила массу времени, по-прежнему требует колоссальных средств и разрешения ее пока не видно.

InBase – ЕЯ оболочка для СУБД и Интернета.

Уникальная технология **INBASE** позволяет создать для прикладной базы данных интерфейс, понимающий произвольные запросы на естественном языке и обеспечивающий прямой доступ к данным для непрофессионального пользователя (руководителя, чиновника, рядового гражданина). Оболочка легко переносится на любой естественный язык. В сочетании с системами распознавания голоса может послужить основой интерфейсов, понимающих устные запросы/сообщения/команды пользователя. Технология ориентирована на широкое применение - внедрение естественно-языковых интерфейсов в деятельности предприятий и организаций любого типа и размера, на всех уровнях административного управления, в интеллектуальных системах Интернет, в частности, в системах электронной коммерции.

InBase-Online. Сотовые телефоны

Данная поисковая система позволяет подбирать модели сотовых телефонов по их характеристикам, а также сравнивать модели. В базу данных занесены характеристики около 70 наиболее популярных аппаратов.

Российский НИИ Искусственного интеплекта.

Описание:

- **Параметры, которые заданы для каждой модели:**

Цена, Вес и размеры, Батарея, Дисплей, Размер адресной книги, Кол-во мелодий, игр, Наличие модема, WAP, ИК-порта, синхронизации с PC, виброзвонка, будильника.

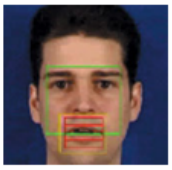
- **Примерные варианты запросов:**

Работа дольше 10 суток, тоньше 2 см

Взаимодействие человека и компьютера.

Понимание жестов.

Digital Lip Reader



Система Intel изолирует движения рта (красный цвет)

Распознавание речи – это многообещающая технология, которая только начинает развиваться. Но на сегодняшний день даже лучшие технологии становятся провальными, когда человек находится в шумном месте. Чтобы исправить эту проблему, разработчики добавили функцию чтения по губам.

Нейронные сети для определения цвета кожи.

- Способность человека отличать один предмет от другого – это сложный процесс, который занял больше миллиона лет. Эта система может распознавать лицо и движения рук даже когда одни предметы передвигаются среди других.
- Исследователи из Китайского Института Современной Оптики работают над использованием цвета кожи для распознавания рук и лица. Это труднее, чем кажется, т.к. цвет обычно меняется в зависимости от освещения.
- Разработчики системы используют камеру, соединенную с процессором, использующий нейронные сети для определения цвета кожи, затем по обработанной информации определяется, какие объекты следует соединить вместе.
- Тестирование показало, что система распознает с точностью до 96.25%.
- Метод распознавания жестов на практике используется в течение 5 лет. А эта работа опубликована в августе 2003 года.

Будущее:

В настоящее время компания Intel занимается компьютерным зрением, что со временем позволит управлять компьютером жестами.

Взаимодействие человека и компьютера.

Распознавание речи.

Основные проблемы перспективы и применения систем речевого ввода текстов:

- Пока компьютер не способен анализировать синтаксическую, семантическую и прагматическую информацию, содержащуюся в высказывании.
- спонтанная речь произносится со средней скоростью 2,5 слов в секунду, профессиональная машинопись - 2 слова в секунду, непрофессиональная - 0,4. Однако оценка средней скорости диктовки в реальных условиях снижается до 0,5-0,8 (в связи с необходимостью четкого произнесения слов при речевом вводе и достаточно высоким процентом ошибок распознавания, нуждающихся в корректировке)
- Даже профессионального диктора может не обрадовать перспектива в течение нескольких часов диктовать малопонятливому и немому компьютеру.
- Печатать на клавиатуре оператор учится в среднем 1-2 месяца. Постановка правильного произношения может занять несколько лет + доп. напряжение и заболевания связок.
- необходимость работать в звукоизолированном отдельном помещении либо пользоваться также звукоизолированным шлемом. Иначе помехи работе своих соседей по офису, которые, в свою очередь, создавая дополнительный шумовой фон, будут значительно затруднять работу речевого распознавателя.

Существующие продукты:

На данный момент лучший - Dragon NaturallySpeaking:

продолжительная речь – это когда вы можете говорить с такой скоростью, как в обычном диалоге и сказанные слова тут же появляются на экране компьютера с точностью до 99%. Dragon NaturallySpeaking использует «натуральную речь», что устраняет необходимость вставлять паузу после каждого слова. Это быстрее, чем печатать. Может сразу помещать текст в Word. Реализован на английском, испанском и французском языке.

Характеристики:

- Активный словарь: (слов) 62 000 слов;
- Обучение: отлично
- Процент правильно распознаваемых слов при диктовке: очень хорошо
- Редактирование : удовлетворительно
- Форматирование: очень хорошо
- Работа с внешними программами: удовлетворительно
- Управление Рабочим столом: удовлетворительно

Плюсы: самая высокая безошибочность распознавания, простота использования.

Минусы: Неудобный ввод чисел, посредственное управление экраном. Нет распознавания Русского языка.

Взаимодействие человека и компьютера.

Распознавание печатных текстов.

Система оптического распознавания печатного текста

Сканер передает изображение в систему OCR (optical character recognition), затем начинается сегментирование. Если текст под наклоном или перевернут вверх ногами, программа его выправляет. Анализируя изображение, система OCR делит его на участки. Одни будут преобразовываться в текст; другие (в которых, например, располагаются картинки) будут оставлены без изменений; третьи участки содержат таблицы, поэтому при их обработке включатся специальные модули. В большинстве систем распознавания возможна как автоматическая сегментация, так и ручная. Допустим, программа ошиблась в анализе структуры документа, выделила таблицу как картинку - вы можете откорректировать результат. Далее разбитый на участки документ поступает на распознавание. Распознавание текста начинается с выделения на изображении (или его части) строк, затем слов и наконец символов. Каждый символ идентифицируется. Система OCR хранит знания о символах в виде эталонов, с которыми сравнивает выделенный объект. Наиболее подходящий эталон и будет соответствовать нашему символу.

Система OCR может работать в пакетном режиме: сначала сканируются все листы, а затем запускается распознавание, которое может работать круглосуточно, без перерывов.

Распознавание печатных текстов компьютером - область, сегодня достаточно хорошо исследованная. Существующие системы обладают высокой точностью распознавания: более 99,9% на текстах хорошего и среднего качества печати.

Пример – FineReader от ABBYY.

Распознавание рукописного текста

- Основная проблема распознавания рукописного текста: на распознавание приходится лишь 30% сложности, а на 70% - задача в области понимания компьютером смысла документа.
- Самая удачная разработка в этой области - язык Graffiti, который основан на печатных английских буквах, но с некоторыми особенностями, облегчающими распознавание букв и минимизирующими число элементов, из которых они состоят. Graffiti требует определенного обучения, но позволяет устройствам с относительно слабым процессором довольно хорошо распознавать текст.

Windows Journal (Tablet PC)

Недостатки: распознавание букв довольно часто работает некорректно, в то время как цифры распознаются уверенно.

Все, что написано на планшете, сохраняется в виде графики (digital ink - "цифровые чернила"). Затем, выделяя требуемую область текста, система распознает написанное. После этого "каракули" превращаются в обычный ASCII текст. Предполагается, что система будет справляться даже с неразборчивым подчерком. Особенностью системы распознавания, предложенной Microsoft, является ее неспособность к обучению, что спорно.

Список литературы.

- http://www.5dt.com/products/pdataglove5.html
- http://www.technologyreview.com
- http://www.synapseadaptive.com/naturallyspeaking/
- http://ocrai.narod.ru/fr.html
- http://msk.nestor.minsk.by/kg/2003/10/kg31009.html
- http://www1.mconline.ru/post/17088/default.asp
- http://neural.narod.ru/Real1.htm
- http://www.inbase.artint.ru/

Приложение 2. Пример презентации на тему «Распознавание образов человека»

РАСПОЗНАВАНИЕ ОБРАЗОВ ЧЕЛОВЕКА

Содержание

Идентификация по форме уха

Области применения биометрии

Российский опыт

Некоторые стоимости вопроса

ИСТОЧНИКИ

Усы, лапы и хвост – вот мои документы! Или кое-что о биометрии

Что такое биометрия?

Биометрия - это методы автоматической идентификации человека и подтверждения личности человека, основанные на физиологических или поведенческих характеристиках.

Биометрия – уникальная, измеримая характеристика человека для автоматической идентификации или верификации.

Из глубины веков

Морфологические признаки с успехом выполняли роль идентификатора личности. Различные народы разрабатывали с этой целью сложные системы нанесения на тело татуировок и рубцов. Позже подтверждением личности стала служить подпись, поставленная от руки. Затем наступила очередь дактилоскопии.

Первое практическое применение – Альфонс Бертильон в конце XIX в.

С 1960-х годов ведет свой отсчет история альтернативных методов опознания.

Идентификация и верификация

Если говорить об идентификации, то система пытается найти, кому принадлежит данный образец, сравнивая образец с базой данных для того, чтобы найти совпадение (также этот процесс называют сравнение «одного ко многим»).

Верификация – это сравнение, при котором биометрическая система пытается верифицировать личность человека. В этом случае, новый биометрический образец сравнивается с ранее сохраненным образцом. Сравнивая эти два образца, система подтверждает, что этот человек действительно тот, за кого он себя выдает.

Идентификационная система спрашивает: «Вы кто?». Верификационная система спрашивает «Вы действительно тот за кого себя выдаете?».

Как это работает

Во-первых, система запоминает образец биометрической характеристики (это и называется процессом записи). Затем полученная информация обрабатывается и преобразовывается в математический код.

Идентификация по любой биометрической системе проходит четыре стадии:

Запись

Выделение

Сравнение

Совпадение/несовпадение

Проблема точности идентификации

Ошибка первого рода (FRR - False Rejection Rate) - это вероятность ложного отказа в доступе клиенту, имеющему право доступа.

Ошибка второго рода (FAR - False Acceptance Rate) - это вероятность ложного доступа, когда система ошибочно опознает чужого как своего.

Биометрические системы также иногда характеризуются *коэффициентом равной вероятности* ошибок 1-го и 2-го рода (EER - Equal Error Rates) представляющим точку совпадения вероятностей FRR и FAR (иногда называемому Crossover Equal Error Rates). Качественная и надежная и система должна иметь низкий уровень EER.

Методы биометрической аутентификации

Статические методы
- По отпечатку пальца
- По форме ладони
- По расположению вен на лицевой стороне ладони
- По сетчатке глаза
- По радужной оболочке глаза
- По форме лица
- По термограмме лица
- По ДНК
- Другие

Динамические методы
- По рукописному почерку
- По клавиатурному почерку
- По голосу
- Другие методы

По показателям ошибок второго рода общая сортировка методов биометрической аутентификации выглядит так (от лучших к худшим):

ДНК;

Радужная оболочка глаза, сетчатка глаза;

Отпечаток пальца, термография лица, форма ладони;

Форма лица, расположение вен на кисти руки и ладони;

Подпись;

Клавиатурный почерк;

Голос.

Сравнение методов по величине ошибок

	отпечатки пальцев	кисть	монокулярная реализация	бинокульрная реализация	сетчатка
FRR	0,01%	0,01%	0,2%	0,01%	0,01%
FAR	0,001%	0,0001%	0,01%	0,001%	0,0001%

Биометрические технологии

Идентификация по отпечаткам пальцев.

Отпечатки пальцев каждого человека уникальны по своему рисунку. Отпечатки пальцев не совпадают у одного человека на разных пальцах, даже у близнецов. В основе указанной технологии лежит уникальность рисунка паппилярных линий на пальце и ладони. Основной принцип данной технологии - сканирование уникального паппилярного узора пальцев специализированным сканером. Время идентификации обычно составляет менее 1 с. Сильная сторона этого способа заключается в ее всемирном одобрении, удобстве и надежности.

Идентификация по лицу. Идентификация личности по лицу может быть произведена различными способами, например, фиксируя изображение в зоне видимости, используя обычную видеокамеру, или с помощью использования теплового рисунка лица. Распознавание освещенного лица заключается в распознавании определенных черт. Используя большое количество камер, система анализирует черты полученного изображения, которые не изменяются на протяжении жизни, не обращая внимания на такие поверхностные характеристики как выражение лица или волосы. Системы идентификации по лицу построены на компьютерных программах, которые анализируют изображения лиц людей с целью их распознавания. Программа измеряет такие характеристики, как расстояние между глазами, длина носа, наклон челюсти и создает некий уникальный файл-шаблон. Может служить эффективным контртеррористическим инструментом, однако в настоящий момент ей недостает точности.

Идентификация по голосу. Использует акустические особенности речи, которые различны и в какой-то мере уникальны. Эти акустические образцы отражают как анатомию (например, размер и форму горла и рта), а также приобретенные привычки (громкость голоса, манера разговора). Преобразование этих образцов в голосовые модели (также называемые отпечатками голоса) наделило данный способ идентификации названием «поведенческая биометрия». Биометрическая технология разбивает каждое произнесенное слово на несколько сегментов. Этот голосовой отпечаток хранится как некий математический код. Для успешной идентификации человека просят ответить на три вопроса. При решении задачи идентификации находится ближайший голос из фонотеки, затем в результате решения задачи верификации подтверждается или опровергается принадлежность фонограммы конкретному лицу. Система практически используется при обеспечении безопасности некоторых особо важных объектов. Достоверность распознавания довольно низкая: уровень EER обычно составляет 2-5%.

Глаз в качестве идентификатора. В настоящий момент в мире наиболее известны две технологии. Они являются одними из наиболее высоконадежных и точных. Первая основана на идентификации рисунка радужной оболочки глаза, окружающей зрачок. Данная характеристика также является уникальной. Видеосистемы смогут идентифицировать человека, даже если он будет в очках или с контактными линзами. Идентификация по радужной оболочке применяется на протяжении нескольких лет, а также была продемонстрирована и опробована на различных этнических группах и национальностях и подтвердила свою надежность и точность. Вторая технология использует метод сканирования глазного дна - сетчатки глаза - и базируется на уникальности углового распределения кровеносных сосудов для каждого человека (компания EyeDentify, терминал Icam 2001).
Более молодая технология идентификации по радужке имеет большие перспективы. Заявленное значение EER= 8,3 x 10-7 свидетельствует о высокой точности метода, однако говорить о результатах пока что рано – будущее покажет.

Идентификация по ладони. Одними из наиболее известных устройств являются биометрические сканеры кисти руки ID-3D компании *Recognition Systems* Inc. (США). Метод идентификации по геометрическим параметрам кисти руки был разработан в 1986г., он основан на сканировании профиля ладони (ширины ладони, пальцев, их длины и толщины, поверхностные области руки). Кисть руки, помещенная на специализированный терминал, сканируется инфракрасным светом, сигнал регистрируется специальной ПЗС-камерой. Считыватель, которому задается конкретный образ ладони, производит сличение оригинала и информации, занесенной ранее в память. Клиент как бы предупреждает считыватель, что будет сканироваться именно его рука, что позволяет многократно уменьшить время идентификации. Одной интересной характеристикой этой технологии является малый объем биометрического образца необходимого для идентификации (несколько байтов). Ошибки метода составляют: первого рода 0,01%, второго рода 0,0001%.

Идентификация по подписи. Данная технология имеет широкое распространение, но используется в большей степени в электронной коммерции для организации доступа к компьютерной информации (идентификация пользователей компьютерных сетей, подтверждение платежных операций с клиентами), доступа к корпоративной информации на handheld-устройствах. Она основана на сопоставлении графических параметров подписи. Вероятность ошибки первого рода FRR и вероятность ошибки второго рода FAR обычно зависят от выбранных пороговых значений. Эта технология использует анализ динамичности подписи для идентификации человека. Технология основана на измерении скорости, нажима и стороны наклона в момент подписи.

Конечные решения иногда представляют собой продукт интеграции технологий идентификации по подписи и по голосу.

Идентификация по клавиатурному "почерку". Используется динамика нажатия на клавиши (ритм печатания), основной характеристикой в данной идентификации является временной интервал между моментами нажатий на клавиши и временем ее удержания. Анализирует со скоростью 1000 знаков в минуту. Преимущества этого способа заключаются в том, что для этого нужна только клавиатура, а сам процесс идентификации и верификации происходит прямо на рабочем месте. Данные системы можно разделить на два основных типа в зависимости от их назначения:
- для идентификации пользователя пытающегося получить доступ к вычислительным ресурсам;
- для осуществления незаметного мониторингового контроля уже в процессе работы (если за компьютер сядет другой человек, доступ прервется). Достоверность распознавания довольно низкая - EER составляет 3-4%. Эти системы удобны для проведения скрытой идентификации пользователя. Основная область применения – доступ к вычислительным ресурсам и базам данных в финансовой сфере.

Почему биометрия ?

Биометрия позволяет идентифицировать вас с помощью вас самих же.

Биометрия предлагает быстрый, удобный, точный, надежный и не очень дорогой способ идентификации с огромным количеством самых разнообразных применений.

Идентификация по отпечаткам пальцев

Идентификация по отпечаткам пальцев - на сегодня самая распространенная биометрическая технология, доля систем распознавания по отпечаткам пальцев составляет 52%.

Доподлинно известно, что в Древнем Вавилоне и Китае оттиски пальцев делали на глиняных табличках и печатях, а в XIV веке в Персии отпечатками пальцев «подписывали» различные государственные документы. Это говорит о том, что уже в то время было отмечено: отпечаток пальца - уникальная характеристика человека, по которой его можно идентифицировать.

Примеры археологических находок, содержащих элементы отпечатков пальцев

Следующий этап развития технологии - начало ее использования в криминалистике, к середине XIX века были сделаны первые предположения об уникальности отпечатков пальцев каждого человека и попытки классификации их по различным участкам папиллярного узора. К концу XIX века появились первые алгоритмы сравнения отпечатков пальцев. В последующие 25 лет «система Генри» прошла адаптацию для использования на государственном уровне в различных странах и примерно с 1925 г. начала широко применяться в криминалистике по всему миру.

Однако, несмотря на широкое распространение методики распознавания отпечатков пальцев для идентификации человека, в первую очередь в криминалистике, до сих пор научно не доказано, что рисунок папиллярного узора пальца человека - абсолютно уникальная характеристика. И хотя за всю более чем столетнюю историю использования этой технологии в криминалистике и других областях не возникло ситуации, когда нашлось бы два человека с абсолютно одинаковыми отпечатками пальцев, уникальность отпечатков - это все же эмпирическое наблюдение.

Сканирование отпечатков пальцев

Все существующие сканеры отпечатков пальцев по используемым ими физическим принципам можно разделить на три группы:

оптические;

кремниевые;

ультразвуковые.

Оптические сканеры - основаны на использовании оптических методов получения изображения (используется эффект нарушенного полного внутреннего отражения; оптоволоконные сканеры; электрооптические сканеры; оптические протяжные сканеры; роликовые сканеры; бесконтактные сканеры). Оптические сканеры не устойчивы к муляжам и мертвым пальцам.

Полупроводниковые сканеры - в их основе лежит использование для получения изображения поверхности пальца свойств полупроводников, изменяющихся в местах контакта гребней папиллярного узора с поверхностью сканера. В настоящее время существует несколько технологий реализации полупроводниковых сканеров (емкостные сканеры; чувствительные к давлению сканеры; термо-сканеры; радиочастотные сканеры; протяжные термо-сканеры). Отметим основные недостатки полупроводниковых сканеров:

сканеры, в частности, чувствительные к давлению, дают изображение низкого разрешения и маленького размера;

необходимость прикладывания пальца непосредственно к полупроводниковой поверхности (так как любой промежуточный слой влияет на результаты сканирования) ведет к ее быстрому изнашиванию;

чувствительность к сильным внешним электрическим полям, которые могут вызвать электростатические разряды, способные вывести сенсор из строя (относится в первую очередь к емкостным сканерам);

большая зависимость качества изображения от скорости движения пальца по сканирующей поверхности присуща прокаточным сканерам.

Ультразвуковые сканеры — данная группа в настоящее время представлена всего одним методом сканирования, который так и называется.

Ультразвуковое сканирование - это сканирование поверхности пальца ультразвуковыми волнами.

Данный способ практически полностью защищен от муляжей, поскольку позволяет кроме отпечатка пальца получать и некоторые дополнительные характеристики о его состоянии (например, пульс внутри пальца). Основные недостатки ультразвуковых сканеров - это:

высокая цена по сравнению с оптическими и полупроводниковыми сканерами;

большие размеры самого сканера.

Кожа человека состоит из двух слоев:

эпидермиса (epidermis), наружного слоя;

дермы (derma), более глубокого слоя.

Складки, видимые на поверхности кожи невооруженным глазом, называются папиллярными линиями (от лат. papillae – сосочки) и отделяются друг от друга неглубокими бороздками. На вершинах складок - гребнях папиллярных линий находятся многочисленные мельчайшие поры. Папиллярные линии на поверхности пальцев рук, образуют различные узоры, называемые папиллярными узорами.

Окончательно папиллярный узор на поверхности пальцев формируется к 7 месяцу внутриутробного развития. С этого времени бороздки, сформировавшиеся на поверхности пальцев, остаются неизменными в течение всей жизни человека.

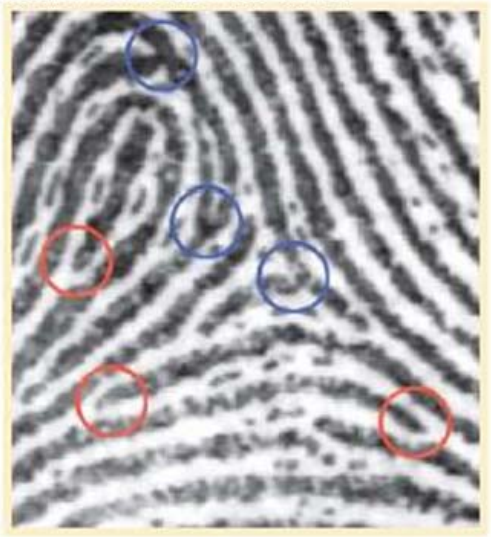
В Российской традиционной дактилоскопии, папиллярные узоры пальцев рук делятся на три основных типа: дуговые (около 5% всех отпечатков), петлевые (65%) и завитковые (30%).

Методы распознавания

В автоматизированных системах используют всего два типа деталей узора (особых точек):

конечные точки – точки, в которых «отчетливо» заканчиваются папиллярные линии;

точки ветвления – определяются как точки, в которых папиллярные линии раздваиваются.



Точки ветвления (○) и конечные точки (○)

Если есть возможность получить изображение поверхности пальца с разрешением около 1000 dpi, на нем можно обнаружить детали внутреннего строения самих папиллярных линий, в частности, поры потовых желез (рисунок 2, пустыми кружками отмечены поры, черными кружками отмечены конечные точки и точки ветвления) и соответственно использовать уже их расположение в целях идентификации. Однако этот метод мало распространен из-за сложности получения в не лабораторных условиях изображений такого качества.

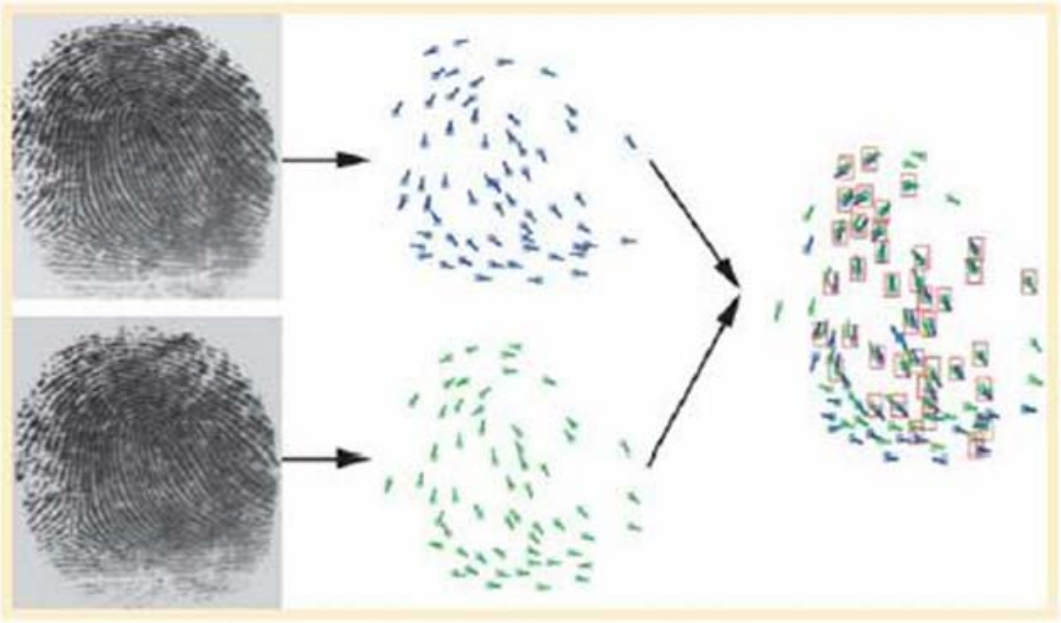
Пустыми кружками отмечены поры, черными — конечные точки и точки ветвления

В настоящее время выделяют три класса алгоритмов сравнения отпечатков пальцев:

1. *Корреляционное сравнение* - два изображения отпечатка пальца накладываются друг на друга, и подсчитывается корреляция (по уровню интенсивности) между соответствующими пикселями вычисленная для различных выравниваний изображений друг относительно друга (например, путем различных смещений и вращений); По соответствующему коэффициенту принимается решение об идентичности отпечатков.
   Вследствие сложности и длительности работы данного алгоритма, особенно при решении задач идентификации (сравнение «один-ко-многим») – системы, построенные с его использованием, сейчас практически не используются.

2. *Сравнение по особым точкам* – по одному или нескольким изображениям отпечатков пальцев со сканера формируется шаблон, представляющий собой двухмерную поверхность, на которой выделены конечные точки и точки ветвления. При сравнении – на отсканированном изображении отпечатка также выделяются эти точки, карта этих точек сравнивается с шаблоном и по количеству совпавших точек принимается решение по идентичности отпечатков (Рисунок 3). В работе алгоритмов данного класса также используются механизмы корреляционного сравнения, но при сравнении положения каждой из предположительно соответствующих друг другу точек.

В силу простоты реализации и скорости работы – алгоритмы данного класса являются наиболее распространенными. Единственным существенным недостатком данного метода сравнения является – достаточно высокие требования к качеству получаемого изображения (около 500 dpi).



Сравнение двух отпечатков пальцев по особым точкам

3. ***Сравнение по узору*** – в данном алгоритме сравнения используется непосредственно особенности строения папиллярного узора на поверхности пальцев. Полученное со сканера изображение отпечатка пальца, разбивается на множество мелких ячеек как показано на рисунке 4 (размер ячеек зависит от требуемой точности).

Разбиение папиллярного узора на ячейки

Расположение линий в каждой ячейке описывается параметрами некоторой синусоидальной волны (Рисунок 5), то есть, задается начальный сдвиг фазы (δ), длина волны (λ) и направление ее распространения (θ).

Соответственно при получении отпечатка для сравнения – он выравнивается и приводится к такому же виду, что и шаблон. Затем сравниваются параметры волновых представлений соответствующих ячеек.

Преимуществом алгоритмов этого класса является то, что данные алгоритмы сравнения не требует получения изображения высокого качества. Отдельно стоит заметить, что в автоматизированной идентификации существует несколько проблем связанных со сложностью сканирования и распознавания некоторых типов отпечатков пальцев, в первую очередь это касается маленьких детей, так как их пальцы очень маленькие, для того, чтобы даже на хорошем оборудовании получить их отпечатки пальцев с детализацией, приемлемой для распознавания. Кроме этого, около 1% взрослых людей, являются обладателями настолько уникальных отпечатков пальцев, что работы с ними приходится или разрабатывать специализированные алгоритмы обработки или делать исключение в виде персонального для них отказа от биометрии.

Волновое представление линий в ячейке

Ошибка первого рода 0,01%

Ошибка второго рода 0,001%

Недостатки метода:

- Системы чувствительны к загрязнениям
- Плохо распознаются отпечатки при сухой коже
- У людей азиатского происхождения слабо выражен папиллярный рисунок. При их включении в базу ошибка первого рода достигает 10-20%
- Большинство людей негативно относится к предъявлению отпечатков пальцев (хотя разработчики утверждают, что в памяти хранится лишь идентификационный код, по которому невозможно восстановить папиллярный узор)

Подходы к защите от муляжей

Обобщенно все методы можно разделить на две группы:

1. Технические – методы защиты, реализованные либо на уровне программного обеспечения, работающего с изображением, либо на уровне считывающего устройства. Рассмотрим их подробнее:

   защита на уровне считывающего устройства: в самом сканере реализован алгоритм получения изображения, который позволяет получить отпечаток пальца только с живого пальца, а не с муляжа, например, так работают оптоволоконные сканеры;

   защита по дополнительной характеристике.

   защита по предыдущим данным.

2. Организационные – организация процессов аутентификации, т.о., чтобы затруднить или исключить возможность использования муляжа.

   Усложнение процесса идентификации. Метод заключается в том, что в процессе регистрации отпечатков пальцев в системе на каждого пользователя регистрируется несколько пальцев (в идеале все 10). После этого непосредственно в процессе аутентификации у пользователя запрашиваются для проверки несколько пальцев в произвольной последовательности, что значительно затрудняет вход в систему по муляжу;

   Мультибиометрия: для аутентификации используется несколько биометрических технологий, например отпечаток пальца и форма лица или сетчатка глаза и т.д.

   Многофакторная аутентификация: суть метода проста – использовать для усиления защиты совокупность методов аутентификации.

Идентификация личности по рисунку радужной оболочки глаза

Идеальна для использования в следующих условиях:

- Помещения для хранения офисных материалов и данных, сейфы, рабочие офисы, оборудованные системами безопасности помещения для проведения деловых встреч и переговоров.
- Лаборатории и заводские цеха.
- Финансовые учреждения.
- Жизненно важные сооружения и коммуникации.
- Центры контроля дорожного движения.
- Аэропорты и портовые сооружения.

Система идентификации личности "один взгляд"

Преимущества использования данной системы идентификации личности:

- Отпадает необходимость в идентификационных карточках или использовании паролей
- Система может быть легко адаптирована к постоянному возрастанию числа пользователей
- Большая экономия времени и затрат
- Как работает технология идентификации личности по рисунку радужной оболочки глаза
- Характеристики радужной оболочки
- Доля ошибок составляет менее 1/1200000
- Отсутствие физического контакта делает эту систему особо безопасной
- Мониторинг состояния доступа и регистрации данных может осуществляться в режиме реального времени

Идентификация по форме уха

Многое из того, что известно об ухе как объекте для идентификации, разработано Ианнарелли и именно его идентификационная система чаще всего используется. По этой системе уши разделяются на четыре формы: овальная, круглая, прямоугольная и треугольная. Форма уха дольше других сохраняется после смерти. Работа системы начинается с составления своеобразного "отпечатка" уха. Компьютер подводит изображение под определенный стандарт. Затем "отпечаток" сравнивается с уже имеющимся в базе данных. Так как идентификация по форме уха пока не имеет широкого распространения, она может рассматриваться как второстепенный уровень идентификации, когда глаза и лицо не могут в достаточной мере служить для идентификации.

Глаз быстрее и точнее

По данным IBG, 52% биометрических устройств на мировом рынке - это устройства распознавания отпечатков пальцев. Характерно, что стоимость устройств, способных сканировать отпечатки пальцев, самая низкая: от $50-100. Популярность остальных устройств невелика: 13% рынка - сканеры формы лица, 11,4 - сканеры формы ладони, 7,3 - распознаватели радужной оболочки глаза, 4,1 - распознаватели голоса, 2,4 - сканеры подписи, остальные 9,2% - другие устройства. Сетчатки глаза - одна из самых точных биометрических систем идентификации человека. Структура сетчатки глаза такова, что сравнение выполняется очень точно: вероятность того, что в результате распознавания в базе окажутся две одинаковые сетчатки глаза,- около одной десятимиллиардной. Более того, компьютер сравнивает два отпечатка оболочки глаза намного быстрее.

Области применения биометрии

Компьютерная безопасность. В данной области нашли применение следующие технологии распознавания: отпечаток пальца, радужная оболочка глаза, голос, почерк, клавиатурный набор.

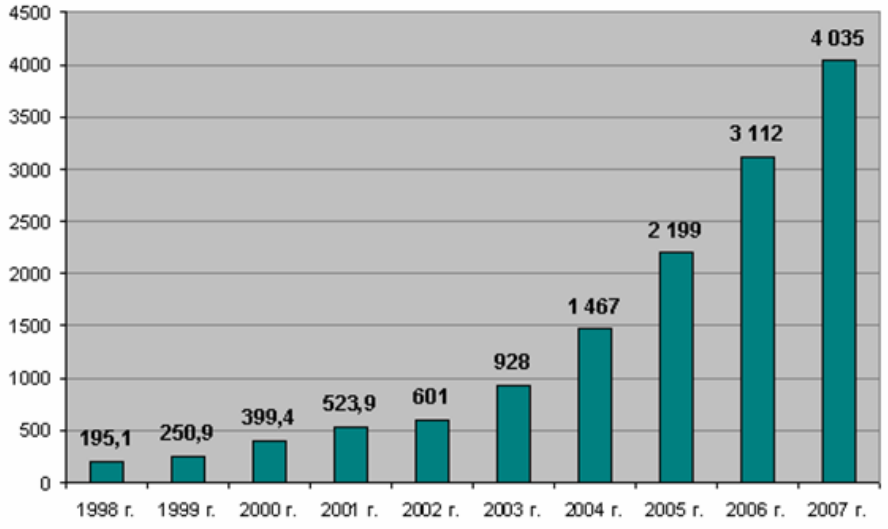
Торговля. Распознавание отпечатка пальца и формы руки.

Системы контроля и управления доступом в помещения. Реализуются следующие технологии распознавания: отпечаток пальца, лицо, форма руки, радужная оболочка глаза, голос.

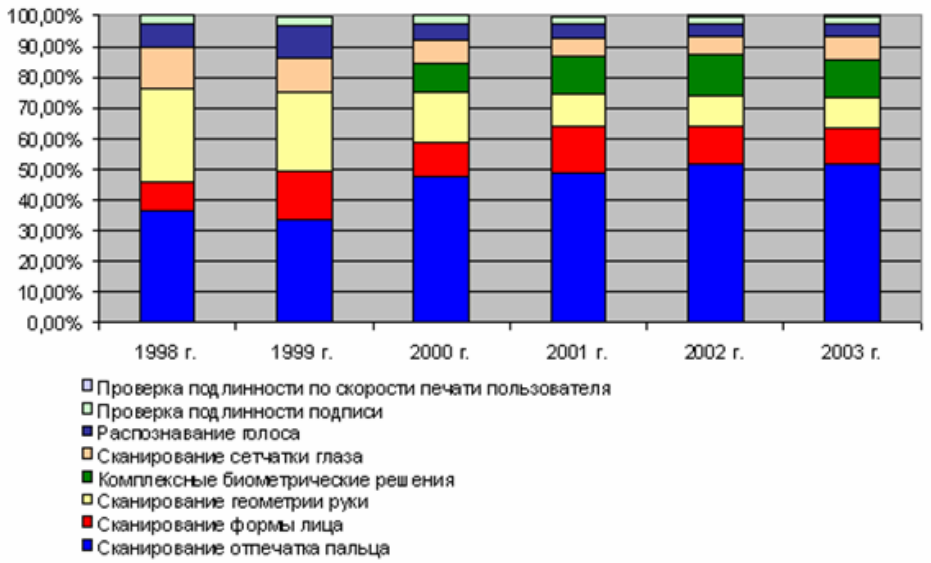
Системы гражданской идентификации и АДИС

Комплексные системы

Объем рынка биометрии в 1998-2007 годах (млн. долл.)



Структура рынка биометрии в 1998-2001 годах



Российский опыт

Одна из отечественных компаний BioLink Technologies предлагает своим клиентам комплексную многоуровневую систему биометрической идентификации пользователя. Ее низший уровень представлен локальными сканерами, установленными на каждом рабочем месте.

Более высокий уровень иерархии системы безопасности представлен специальным сервером Authenteon.

Наконец, для крупных локальных сетей предусмотрено создание кластерных систем безопасности, когда несколько серверов Authenteon работают в единой связке, обеспечивая тем самым высокую масштабируемость и быстродействие.

Некоторые стоимости вопроса

Что клеить в паспорт?

Налогоплательщики заплатят за новые загранпаспорта от 0,4 до 1,5 млрд. долларов. По экспертным оценкам, система идентификации по отпечаткам пальцев в новых загранпаспортах обойдется от 350-400 млн. долларов. В 'Биометрических технологиях' говорят, что себестоимость загранпаспорта с цифровым фото и информацией об отпечатках пальцев не превысит 15 долларов. Если применять чипы с рисунком радужной оболочки глаза, стоимость паспорта вырастет до 50 долларов. Из суммы 500 млн. долларов необходимо потратить на создание единой базы данных паспортно-визовых документов, и еще около 1 миллиарда долларов - на оборудование и изготовление бланков с чипами.

ИСТОЧНИКИ

http://biometrics.ru

http://www.ean.ru/art1/art208.html

http://bastion.kiev.ua/index.php?lang_id=1&content_id=194
http://daily.sec.ru/dailypblshow.cfm?rid=8&pid=4408&pos=1&stp=10&cd=5&cm=6&cy=2002

PC Magazine / Russian Edition №№ 1, 2 2004 год