Биометрическая аутентификация пользователя

Выполнил студент группы КС 1-41 Гришечкин Даниил

Процедуры идентификации и аутентификации

Процедуры идентификации и аутентификации пользователя могут базироваться не только на секретной информации, которой обладает пользователь (пароль, персональный идентификатор, секретный ключ и т. п.). В последнее время все большее распространение получает *биометрическая аутентификация пользователя,* позволяющая уверенно аутентифицировать потенциального пользователя путем измерения физиологических параметров и характеристик человека, особенностей его поведения. Основные достоинства биометрических методов:

- высокая степень достоверности аутентификации по биометрическим признакам (из-за их уникальности);
- неотделимость биометрических признаков от дееспособной личности;
- трудность фальсификации биометрических признаков. Активно используются следующие биометрические признаки:
- отпечатки пальцев;
- геометрическая форма кисти руки;
- форма и размеры лица;
- особенности голоса;
- узор радужной оболочки и сетчатки глаз.

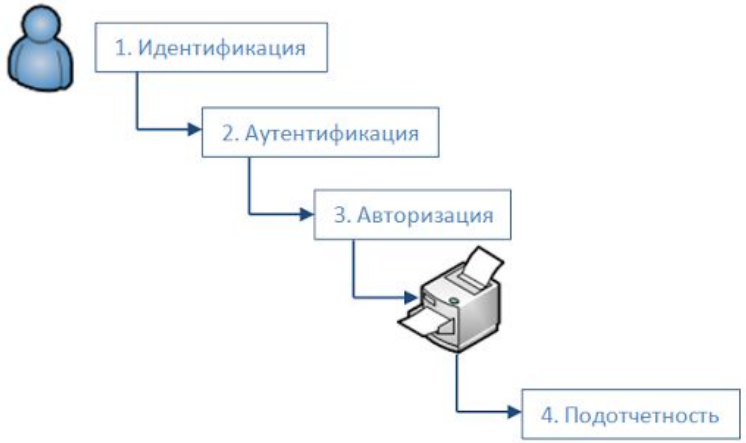
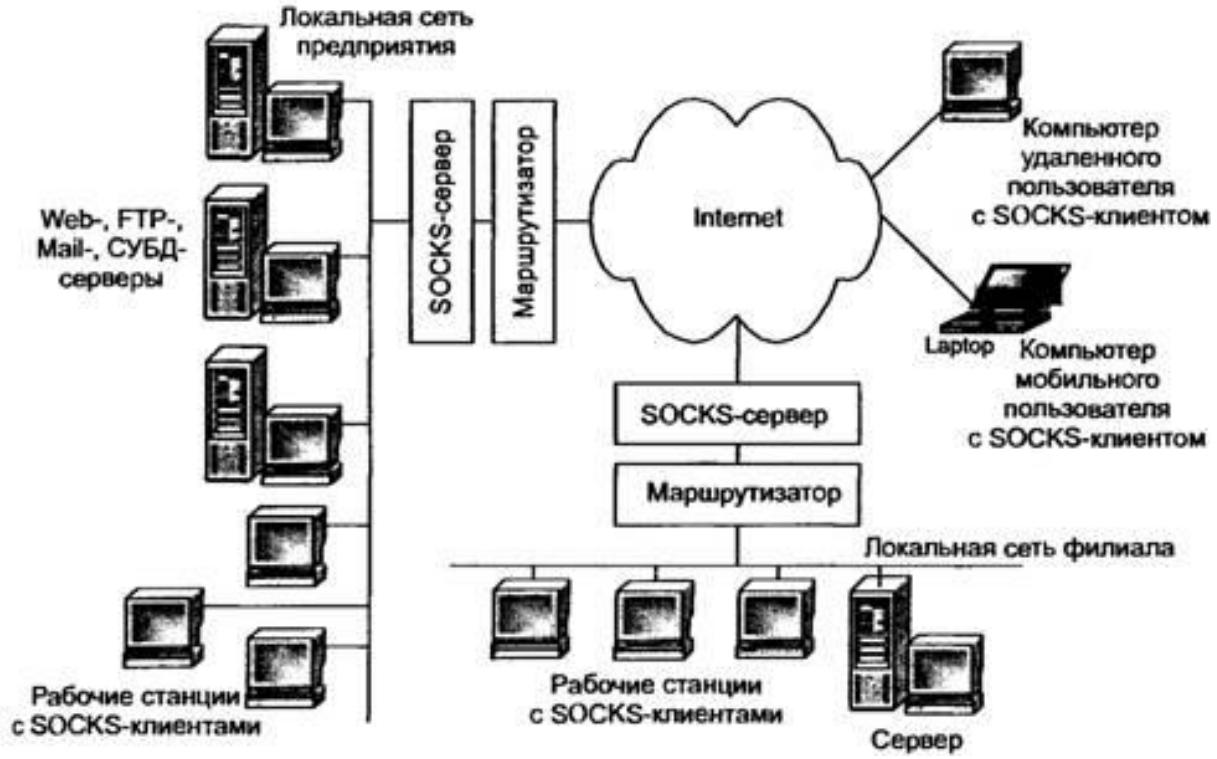


Схема функционирования биометрической подсистемы аутентификации

Рассмотрим типичную схему функционирования биометрической подсистемы аутентификации. При регистрации в системе пользователь должен продемонстрировать один или несколько раз свои характерные биометрические признаки. Эти признаки (известные как подлинные) регистрируются системой как контрольный «образ» (биометрическая подпись) законного пользователя. Этот образ пользователя хранится системой в электронной форме и используется для проверки идентичности каждого, кто выдает себя за соответствующего законного пользователя. В зависимости от совпадения или несовпадения совокупности предъявленных признаков с зарегистрированными в контрольном образе предъявивший их признается законным пользователем (при совпадении) или незаконным (при несовпадении).

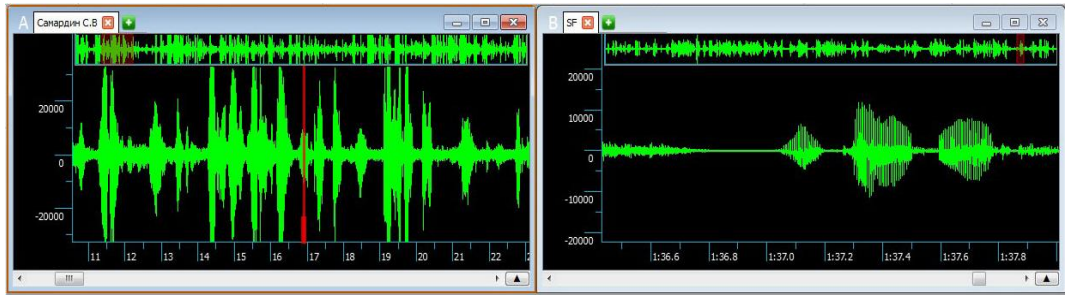


Два параметра эффективности биометрической аутентификационной системы

С точки зрения потребителя, эффективность биометрической аутентификационной системы характеризуется двумя параметрами:

- коэффициентом ошибочных отказов FRR (false-reject rate);
- коэффициентом ошибочных подтверждений FAR (false-alarm rate).

Ошибочный отказ возникает, когда система не подтверждает личность законного пользователя (типичные значения FRR — порядка одной ошибки на 100). *Ошибочное подтверждение* происходит в случае подтверждения личности незаконного пользо вателя (типичные значения FAR — порядка одной ошибкина 10 000). Эти коэффициенты связаны друг с другом: каждому коэффициенту ошибочных отказов соответствует определенный коэффициент ошибочных подтверждений.



В совершенной биометрической системе оба параметра ошибки должны быть равны нулю. К сожалению, биометрические системы тоже не идеальны. Обычно системные параметры настраивают так, чтобы добиться требуемого коэффициента ошибочных подтверждений, что определяет соответствующий коэффициент ошибочных отказов.

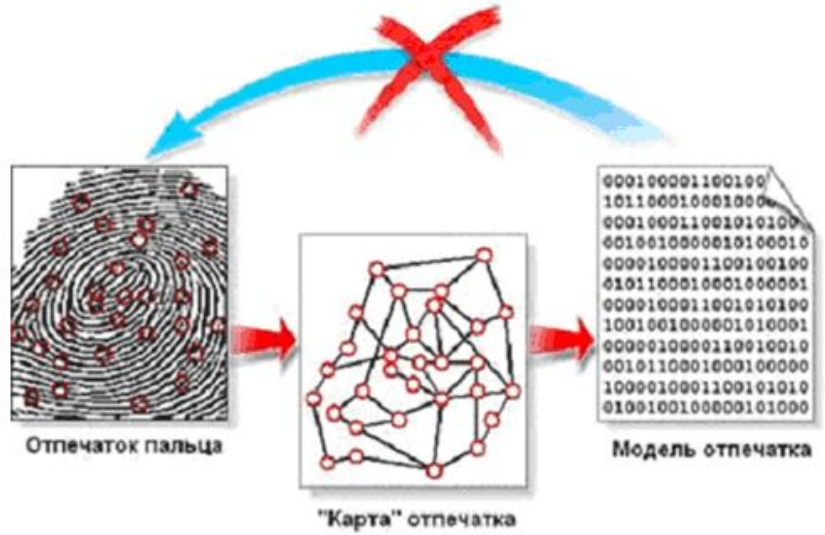
К настоящему времени разработаны и продолжают совершенствоваться технологии аутентификации по отпечаткам пальцев, радужной оболочке глаза, по форме кисти руки и ладони, по форме и размеру лица, по голосу и «клавиатурному почерку».

Чаще всего биометрические системы используют в качестве параметра идентификации отпечатки пальцев (дактилоскопические системы аутентификации). Такие системы просты и удобны, обладают высокой надежностью аутентификации.

Дактилоскопические системы аутентификации

Одна из основных причин широкого распространения таких систем — наличие больших банков данных отпечатков пальцев. Пользователями подобных систем главным образом являются полиция, различные государственные и некоторые банковские организации.

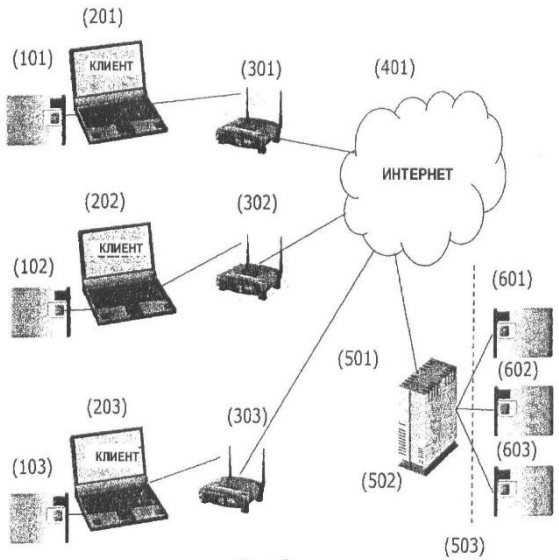
В общем случае биометрическая технология распознавания отпечатков пальцев заменяет защиту доступа с использованием пароля. Большинство систем используют отпечаток одного пальца.



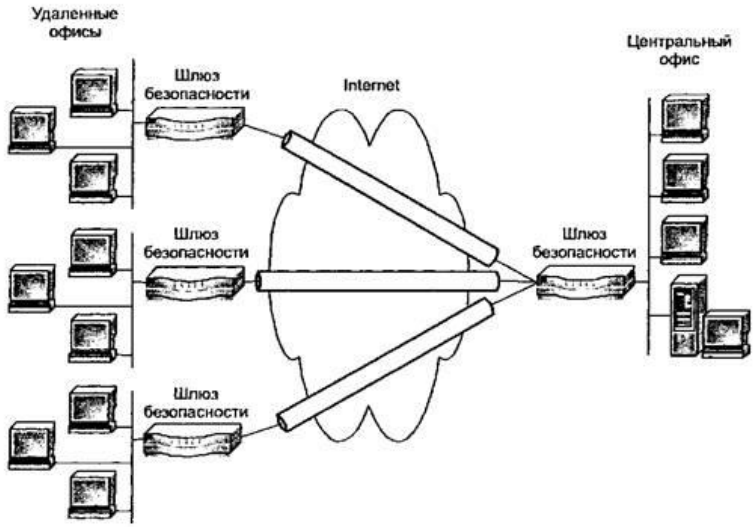
Основные элементы дактилоскопической системы аутентификации

Основными элементами дактилоскопической системы аутентификации являются:

- сканер;
- ПО идентификации, формирующее идентификатор пользователя;
- ПО аутентификации, производящее сравнение отсканированного отпечатка пальца с имеющимися в БД «паспортами» пользователей.



Фиг. 8



Дактилоскопическая система аутентификации работает следующим образом. Сначала проходит регистрация пользователя. Как правило, производится несколько вариантов сканирования в разных положениях пальца на сканере. Понятно, что образцы будут немного отличаться, и поэтому требуется сформировать некоторый обобщенный образец — «паспорт». Результаты запоминаются в БД аутентификации. При аутентификации производится сравнение отсканированного отпечатка пальца с «паспортами», хранящимися в БД.

Задача формирования «паспорта» и задача распознавания предъявляемого образца — это задачи распознавания образов. Для их решения используются различные алгоритмы, являющиеся ноу-хау фирм-производителей подобных устройств.

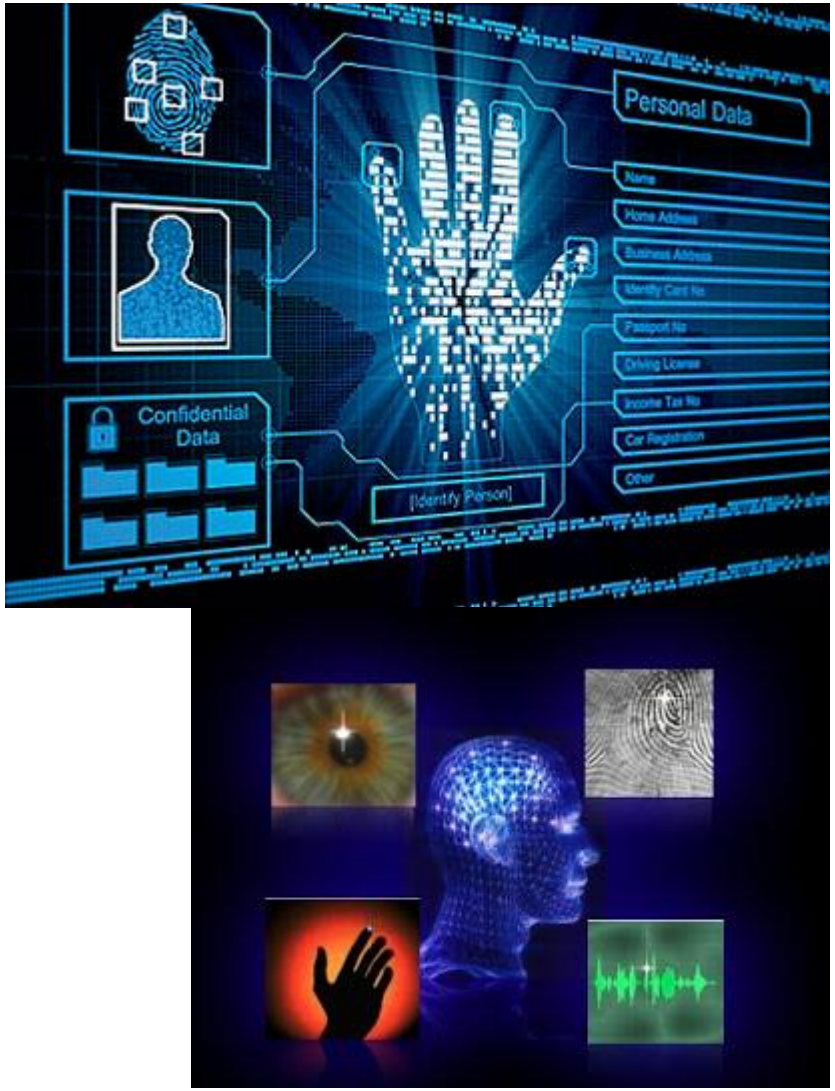
Сканеры отпечатков пальцев

Многие производители **все** чаще переходят от дактилоскопического оборудования на базе оптики к продуктам, основанным на интегральных схемах. Последние имеют значительно меньшие размеры, чем оптические считыватели, и поэтому их проще реализовать в широком спектре периферийных устройств.

Некоторые производители комбинируют биометрические системы со смарт-картами и картами-ключами. Например, в биометрической идентификационной смарт-карте Authentic реализован следующий подход. Образец отпечатка пальца пользователя запоминается в памяти карты в процессе внесения в списки идентификаторов пользователей, устанавливая соответствие между образцом и личным ключом шифрования. Затем, когда пользователь вводит смарт-карту в считыватель и прикладывает палец к сенсору, ключ удостоверяет его личность. Комбинация биометрических устройств и смарт-карт является удачным решением, повышающим надежность процессов аутентификации и авторизации.

Небольшой размер и невысокая цена датчиков отпечатков пальцев на базе интегральных схем превращает их в идеальный интерфейс для систем защиты. Их можно встроить в брелок для ключей, и пользователи получат универсальный ключ, который обеспечит защищенный доступ ко всему, начиная от компьютеров до входных дверей, дверей автомобилей и банкоматов.

Системы аутентификации по форме ладони



Системы аутентификации по форме ладони используют сканеры формы ладони, обычно устанавливаемые на стенах. Следует отметить, что подавляющее большинство пользователей предпочитают системы этого типа.

Устройства считывания формы ладони создают объемное изображение ладони, измеряя длину пальцев, толщину и площадь поверхности ладони. Например, продукты компании Recognition Systems выполняют более 90 измерений, которые преобразуются в 9-разрядный образец для дальнейших сравнений. Этот образец может быть сохранен локально, на индивидуальном сканере ладони либо в централизованной БД.

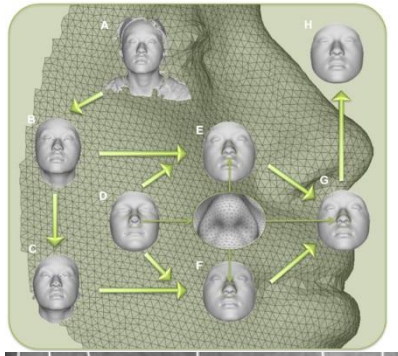
Но уровню доходов устройства сканирования формы ладони, занимают 2-е место среди биометрических устройств, но редко применяются в сетевой среде из-за высокой стоимости и размера. Однако сканеры формы ладони хорошо подходят для вычислительных сред со строгим режимом безопасности и напряженным трафиком, включая серверные комнаты. Они достаточно точны и обладают довольно низким коэффициентом ошибочного отказа **FRR.**

Системы аутентификации по лицу и голосу

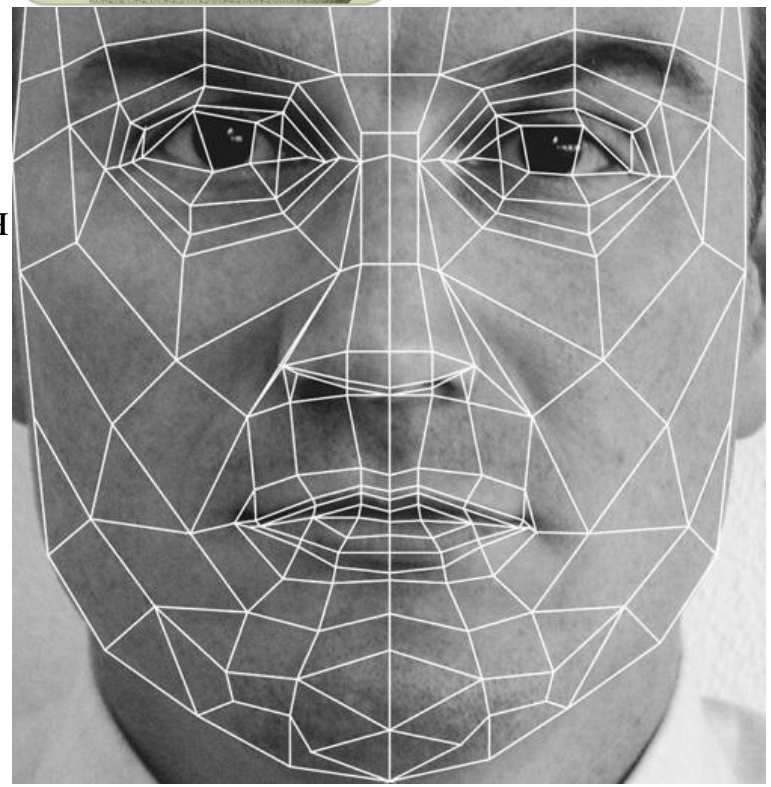
Системы аутентификации по лицу и голосу наиболее доступны из-за их дешевизны, поскольку большинство современных компьютеров имеют видео- и аудиосредства. Системы данного класса применяются при удаленной идентификации субъекта доступа в телекоммуникационных сетях.

Технология сканирования черт лица

Технология сканирования черт лица подходит для тех приложений, где прочие биометрические технологии непригодны. В этом случае для идентификации и верификации личности используются особенности глаз, носа и губ. Производители устройств распознавания черт лица применяют собственные математические алгоритмы для идентификации пользователей

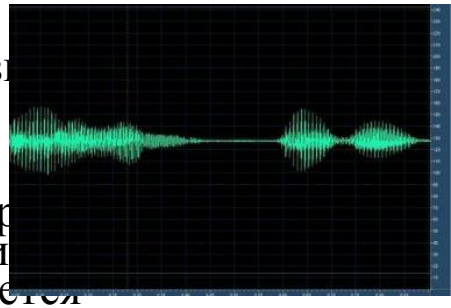


Исследования, проводимые компанией International Biometric Group, говорят о том, что сотрудники многих организаций не доверяют устройствам распознавания по чертам лица. Кроме того, по данным этой компании, сканирование черт лица — единственный метод биометрической аутентификации, который не требует согласия на выполнение проверки (и может осуществляться скрытой камерой), а потому имеет негативный для пользователей подтекст.



Следует отметить, что технологии распознавания черт лица требуют дальнейшего совершенствования. Большая часть алгоритмов распознавания черт лица чувствительна к колебаниям в освещении, вызванным изменением интенсивности солнечного света в течение дня. Изменение положения лица также может повлиять на узнаваемость. Различие в положении в 15 % между запрашиваемым изображением и изображением, которое находится в БД, напрямую сказывается на эффективности: при различии в 45° распознавание становится неэффективным.

Системы аутентификации по голосу



Системы аутентификации по голосу экономически выгодны по тем же причинам, что и системы распоз по чертам лица. В частности, их можно устанавливать с оборудованием (например, микрофонами), поставляемым в стандартной комплектации со многими ПК.

Системы аутентификации по голосу при записи образца и в процессе последующей идентификации опир на такие особенности голоса, как высота, модуляция и частота звука. Эти показатели определяются физи характеристиками голосового тракта и уникальны для каждого человека. Распознавание голоса применяется вместо набора номера в определенных системах Sprint. Технология распознавания голоса отличается **от** распознавания речи: последняя интерпретирует то, что говорит абонент, а технология распознавания голоса абонента подтверждает личность говорящего.

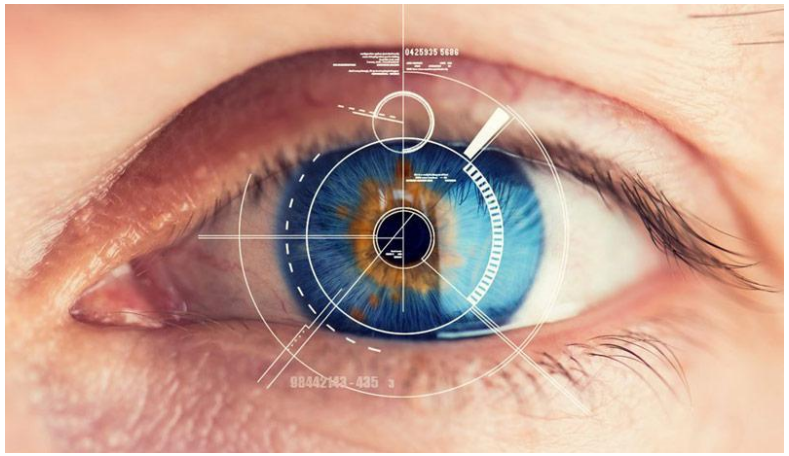
Поскольку голос можно просто записать на пленку или другие носители, некоторые производители встраивают в свои продукты операцию запроса отклика. Эта функция предлагает пользователю при входе ответить на предварительно подготовленный и регулярно меняющийся запрос, например такой: «Повторите числа 0, 1, 3».

Оборудование аутентификации по голосу более пригодно для интеграции в приложения телефонии, чем для входа в сеть. Обычно оно позволяет абонентам получить доступ в финансовые или прочие системы посредством телефонной связи.

Технологии распознавания говорящего имеют некоторые ограничения. Различные люди могут говорить похожими голосами, а голос любого человека может меняться со временем в зависимости от самочувствия, эмоционального состояния и возраста. Более того, разница в модификации телефонных аппаратов и качество телефонных соединений могут серьезно усложнить распознавание.

Поскольку голос сам по себе не обеспечивает достаточной точности, распознавание по голосу следует сочетать с другими биометриками, такими как распознавание черт лица или отпечатков пальцев.

Системы аутентификации по узору радужной оболочки и сетчатки глаз



Системы аутентификации по узору радужной оболочки и сетчатки глаз могут быть разделены на два класса:

- использующие рисунок радужной оболочки глаза;
- использующие рисунок кровеносных сосудов сетчатки глаза.

Сетчатка человеческого глаза представляет собой уникальный объект для аутентификации. Рисунок кровеносных сосудов глазного дна отличается даже у близнецов. Поскольку вероятность повторения параметров радужной оболочки и сетчатки глаза имеет порядок 1(Г78, такие системы являются наиболее надежными среди всех биометрических систем и применяются там, где требуется высокий уровень безопасности (например, в режимных зонах военных и оборонных объектов).

Биометрический подход

Биометрический подход позволяет упростить процесс выяснения «кто есть кто». При использовании дактилоскопических сканеров и устройств распознавания голоса для входа в сети сотрудники избавляются от необходимости запоминать сложные пароли. Ряд компаний интегрируют биометрические возможности в системы однократной аутентификации SSO (Single Sign-On) масштаба предприятия. Подобная консолидация позволяет сетевым администраторам заменить службы однократной аутентификации паролей биометрическими технологиями.

Рис. 2. Алгоритм обработки позволяет хранить не само изображение, а его "образ" (набор характерных данных). Данный принцип верен и для других систем биометрической идентификации

Биометрическая аутентификация пользователя

Биометрическая аутентификация пользователя может быть использована при *шифровании* в виде модулей блокировки доступа к секретному ключу, который позволяет воспользоваться этой информацией только истинному владельцу частного ключа. Владелец может затем применять свой секретный ключ для шифрования информации, передаваемой по частным сетям или по Internet. Ахиллесовой пятой многих систем шифрования является проблема безопасного хранения самого криптографического секретного ключа. Зачастую доступ к ключу длиной 128 разрядов (или даже больше) защищен лишь паролем из 6 символов, т. е. 48 разрядов. Отпечатки пальцев обеспечивают намного более высокий уровень защиты и, в отличие от пароля, их невозможно забыть.