Содержание:

Введение

Для идентификации личности современные электронные систем контроля и управления доступом (СКУД) используют устройства нескольких типов. Наиболее распространенными являются:

- кодонаборные устройства ПИН-кода (кнопочные клавиатуры);

- считыватели бесконтактных смарт-карт (интерфейс Виганда);

- считыватели проксимити-карт;

- считыватели ключа «тач-мемори»;

- считыватели штрих-кодов;

- биометрические считыватели.

В настоящее время самое широкое распространение получили всевозможные считыватели карт (проксимити, Виганда, с магнитной полосой и т. п). Они имеют свои неоспоримые преимущества и удобства в использовании, однако при этом в автоматизированном пункте доступа контролируется «проход карточки, а не человека». В то же время карточка может быть потеряна или украдена злоумышленниками. Все это снижает возможность использования СКУД, основанных исключительно на считывателях карт, в приложениях с высокими требованиями к уровню безопасности. Несравненно более высокий уровень безопасности обеспечивают всевозможные биометрические устройства контроля доступа, использующие в качестве идентифицирующего признака биометрические параметры человека (отпечаток пальца, геометрия руки, рисунок сетчатки глаза и т. п.), которые однозначно предоставляют доступ только определенному человеку - носителю кода (биометрических параметров). Но на сегодняшний день подобные устройства все еще остаются достаточно дорогими и сложными, и поэтому находят свое применение только в особо важных пунктах доступа. Считыватели штрих-

кодов в настоящее время практически не устанавливаются, поскольку подделать пропуск чрезвычайно просто на принтере или на копировальном аппарате.

Цель работы рассмотреть принципы работы и использования биометрических средств иденфикации личности.

1. Классификация и основные характеристики биометрических средств идентификации личности

Достоинства биометрических идентификаторов на основе уникальных биологических, физиологических особенностей человека, однозначно удостоверяющих личность, привели к интенсивному развитию соответствующих средств. В биометрических идентификаторах используются статические методы, основанные на физиологических характеристиках человека, т. е. на уникальных характеристиках, данных ему от рождения (рисунки папиллярных линий пальцев, радужной оболочки глаз, капилляров сетчатки глаз, тепловое изображение лица, геометрия руки, ДНК), и динамические методы (почерк и динамика подписи, голос и особенности речи, ритм работы на клавиатуре). Предполагается использовать такие уникальные статические методы, как идентификация по подноггевому слою кожи, по объему указанных для сканирования пальцев, форме уха, запаху тела, и динамические методы -идентификация по движению губ при воспроизведении кодового слова, по динамике поворота ключа в дверном замке и т. д. Классификация современных биометрических средств идентификации показана на рис. 1.

Биометрические идентификаторы хорошо работают только тогда, когда оператор может проверить две вещи: во-первых, что биометрические данные получены от конкретного лица именно во время проверки, а во-вторых, что эти данные совпадают с образцом, хранящимся в картотеке. Биометрические характеристики являются уникальными идентификаторами, но вопрос их надежного хранения и защиты от перехвата по-прежнему остается открытым

Биометрические идентификаторы обеспечивают очень высокие показатели: вероятность несанкционированного доступа - 0,1 - 0,0001 %, вероятность ложного задержания - доли процентов, время идентификации - единицы секунд, но имеют более высокую стоимость по сравнению со средствами атрибутной идентификации. Качественные результаты сравнения различных биометрических технологий по

точности идентификации и затратам указаны на рис. 2. Известны разработки СКУД, основанные на считывании и сравнении конфигураций сетки вен на запястье, образцов запаха, преобразованных в цифровой вид, анализе носящего уникальный характер акустического отклика среднего уха человека при облучении его специфическими акустическими импульсами и т. д.

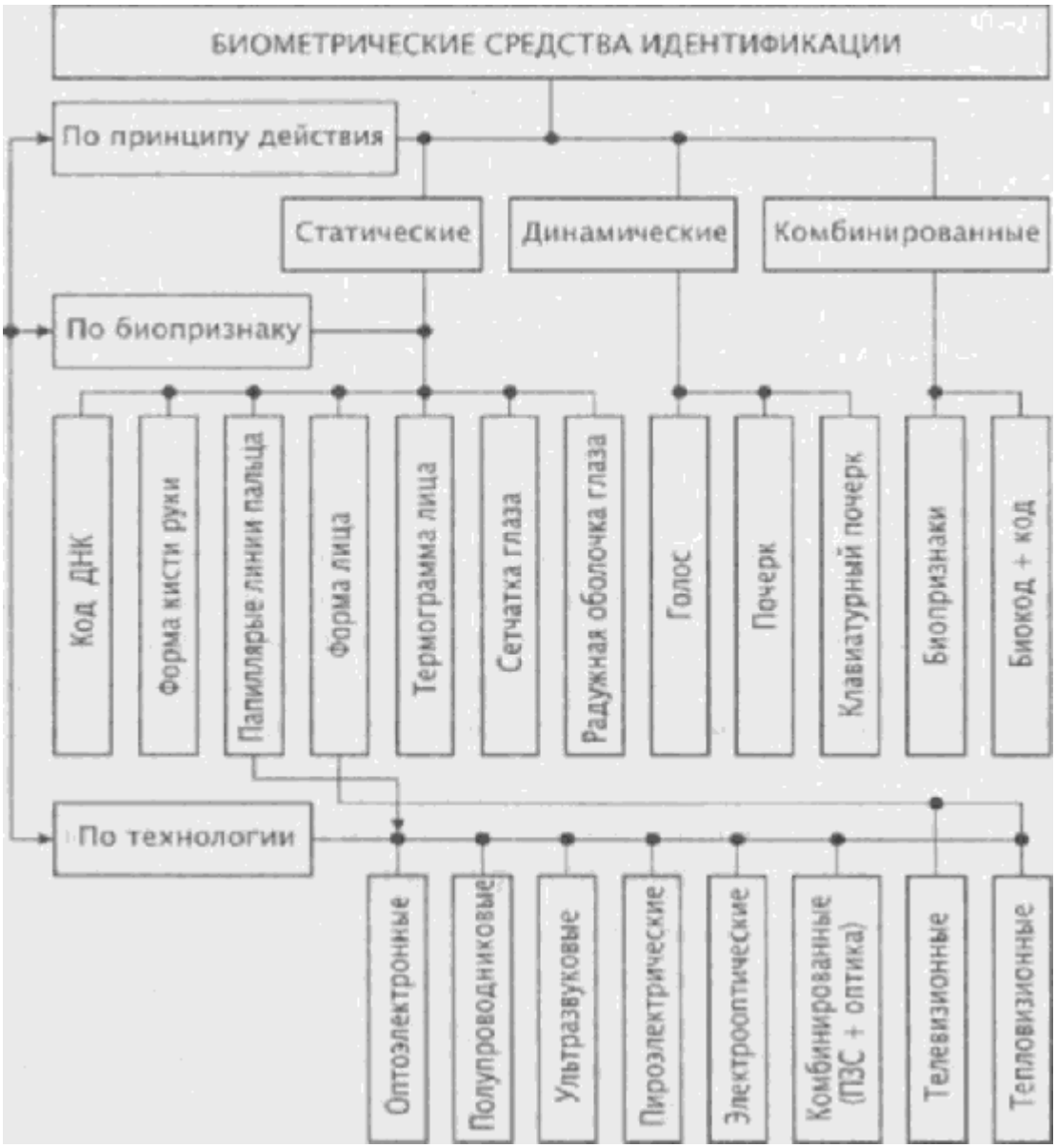


Рис. 1. Классификация современных биометрических средств идентификации

Тенденция значительного улучшения характеристик биометрических идентификаторов и снижения их стоимости приведет к широкому применению биометрических идентификаторов в различных системах контроля и управления доступом. В настоящее время структура этого рынка представля-

тся следующим образом: верификация голоса - 11 %, распознавание лица -15 %, сканирование радужной оболочки глаза - 34 %, сканирование отпечатков пальцев - 34 %, геометрия руки - 25 %, верификация подписи - 3 %.

Любая биометрическая технология применяется поэтапно:

- сканирование объекта;

- извлечение индивидуальной информации;

- формирование шаблона;

- сравнение текущего шаблона с базой данных.

Методика биометрической аутентификации заключается в следующем. Пользователь, обращаясь с запросом к СКУД на доступ, прежде всего, идентифицирует себя с помощью идентификационной карточки, пластикового ключа или личного идентификационного номера. Система по предъявленному пользователем идентификатору находит в своей памяти личный файл (эталон) пользователя, в котором вместе с номером хранятся данные его биометрии, предварительно зафиксированные во время процедуры регистрации пользователя. После этого пользователь предъявляет системе для считывания обусловленный носитель биометрических параметров. Сопоставив полученные и зарегистрированные данные, система принимает решение о предоставлении или запрещении доступа.

2. Особенности реализации статических методов биометрического контроля

2.1 Идентификация по рисунку папиллярных линий

Применение данной технологии получило широкое распространение в системах автоматической идентификации по отпечатку пальца (AFIS).

Весь процесс идентификации занимает не более нескольких секунд и не требует усилий от тех, кто использует данную систему доступа. В настоящее время уже производятся подобные системы размером меньше колоды карт. Определенным недостатком, сдерживающим развитие данного метода, является предубеждение части людей, которые не желают оставлять информацию о своих отпечатках пальцев. При этом контраргументом разработчиков аппаратуры является заверение в том, что информация о папиллярном узоре пальца не хранится - хранится лишь короткий идентификационный код, построенный на базе характерных особенностей отпечатка вашего пальца. По данному коду нельзя воссоздать узор и сравнить его с отпечатками пальцев, оставленными, допустим, на месте преступления. Преимущества доступа по отпечатку пальца - простота использования, удобство и надежность. Хотя процент ложных отказов при идентификации составляет около 3 %, ошибка ложного доступа - меньше 0,00001 % (1 на 1 000 000).

Существует два основных алгоритма сравнения полученного кода с имеющимся в базе шаблоном: по характерным точкам и по рельефу всей поверхности пальца. В первом случае выявляются характерные участки и запоминается их взаиморасположение. Во втором случае запоминается вся «картина» в целом. В современных системах используется также комбинация обоих алгоритмов, что позволяет повысить уровень надежности системы.

Традиционно американские компании занимают лидирующие позиции в разработке биометрических систем безопасности, в этом направлении успешно работают такие фирмы, как Identix, T-Netix, American Biometric Company, National Registry, sagem, Morpho, Verditicom, Infenion. Из российских компаний-разработчиков идентификационных устройств по папиллярным узорам пальцев заслуживает внимания компания «Биолинк».

С целью идентификации личности по рисунку папиллярных линий пальца проверяемый набирает на клавиатуре свой идентификационный номер и помещает указательный палец на окошко сканирующего устройства. При совпадении получаемых признаков с эталонными, предварительно заложенными в память ЭВМ и активизированными при наборе идентификационного номера, подается команда исполнительному устройству. Хотя рисунок папиллярных линий пальцев индивидуален, использование полного набора их признаков чрезмерно усложняет устройство идентификации. Поэтому с целью его удешевления применяют признаки, наиболее легко измеряемые автоматом. Выпускают сравнительно недорогие устройства идентификации по отпечаткам пальцев, действие которых

основано на измерении расстояния между основными дактилоскопическими признаками. На величину вероятности ошибки опознания влияют также различные факторы, в том числе температура пальцев (рис. 3). Кроме того, процедура аутентификации у некоторых пользователей ассоциируется с процедурой снятия отпечатков у преступников, что вызывает у них психологический дискомфорт.

Дактилоскопия построена на двух основных качествах, присущих папиллярным узорам кожи пальцев и ладоней:

- стабильность рисунка узора на протяжении всей жизни человека;

- уникальность рисунка, что означает отсутствие двух индивидуумов с одинаковыми дактилоскопическими отпечатками.

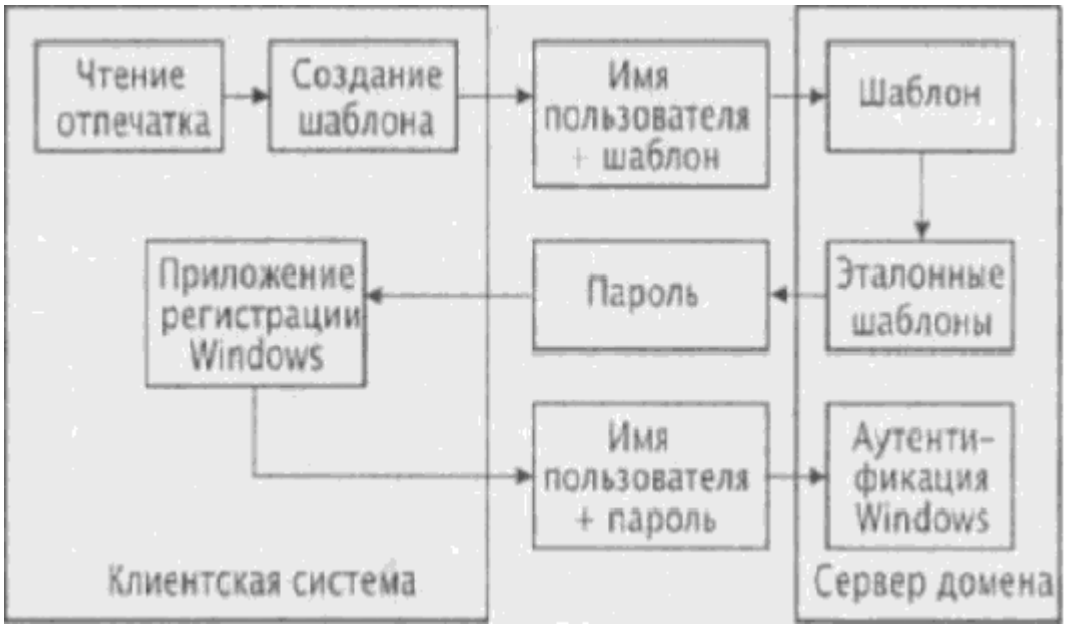


Рис. 2. Процесс аутентификации по отпечаткам пальцев

Распознавание отпечатка пальца основано на анализе распределения особых точек (концевых точек и точек разветвления папиллярных линий), местоположение которых задается в декартовой системе координат.

Для снятия отпечатков в режиме реального времени применяются специальные контактные датчики различных типов. Системы идентификации по отпечаткам пальцев выпускаются в течение почти трех десятков лет Однако благодаря достигнутым успехам в области машинного распознавания отпечатков только в последние годы заметно увеличилось число фирм, выпускающих терминалы персональной аутентификации на базе дактилоскопии.

Американская фирма Fingermatrix предложила терминал Ridge Reader, который благодаря процедуре компенсации различных отклонений, возникающих при снятии отпечатка пальца в реальных условиях, а также применяемому способу «очищения» изображения и восстановления папилярного узора (который может быть «затуманен» из-за наличия на пальце грязи, масла или пота) допускает коэффициент ошибок 1-го рода не более 0,1 %, 2-го рода - не более 0,0001 %. Время обработки изображения составляет 5 с, регистрации пользователя составляет 2-3 мин. Для хранения одного цифрового образа отпечатка (эталона) расходуется 256 байт памяти.

Компания De La Rue Printrak Inc. производит систему PIV-100 на базе терминала аутентификации по отпечаткам пальцев. Кроме этих терминалов, в состав аппаратуры входят центральный процессор, контрольный пульт, дисплей, принтер, накопители на винчестерских дисках (для хранения базы данных), накопители на гибких дисках (для резервной памяти).

В этой системе требуемые коэффициенты ошибок могут выбираться в зависимости от необходимого уровня обеспечения безопасности путем под-стройки внутренних зависимых системных параметров, таких как пороговые значения принятия решения, сопоставляемые характеристики, стратегия распознавания. Но за возросшую точность приходится расплачиваться уменьшением быстродействия и снижением удобств для пользователей. Автоматическая обработка полученного дактилоскопического изображения начинается с преобразования первичного образа с разрешением 512 х 512 точек изображения и плотностью 8 бит на точку к конечному набору (множеству), состоящему примерно из 100 особых точек папиллярного узора, каждая из которых занимает 3 байт памяти. В результате объем памяти для хранения одного отпечатка по сравнению с первоначальным изображением уменьшается примерно в 1000 раз. Сопоставление двух дактилоскопических образов - оригинального и эталонного, хранящегося в памяти системы, - производится с помощью некоторой корреляционной процедуры. Время регистрации пользователя в базе данных - меньше 2 мин; вся процедура проверки пользователя занимает около 10 с, из которых 2 с уходит на аутентификацию, т. е. на вычисления по сопоставлению отпечатков.

Говоря о надежности аутентификационной процедуры по отпечаткам пальцев, необходимо рассмотреть также вопрос о возможности их копирования и использования другими лицами для получения несанкционированного доступа. В качестве одной из возможностей по обману терминала специалисты называют изготовление искусственной кисти с требуемыми отпечатками пальцев (или

изъятия «подлинника» у законного владельца). Но существует и способ борьбы с такой фальсификацией. Для этого в состав терминального оборудования должны быть включены инфракрасный детектор, который позволит зафиксировать тепловое излучение от руки (или пальца), и (или) фотоплетизмограф, который определяет наличие изменений отражения света от поверхности потока крови.

Другим способом подделки является непосредственное нанесение папиллярного узора пальцев законного пользователя на руки злоумышленника с помощью специальных пленок или пленкообразующих составов. Такой способ довольно успешно может быть использован для получения доступа через КПП. Однако в этом случае необходимо получить качественные отпечатки пальцев законного пользователя, причем именно тех пальцев, которые были зарегистрированы системой, и именно в определенной последовательности (например, если система настроена на проверку не одного, а двух и более пальцев по очереди), но эта информация неизвестна законному пользователю и, следовательно, он не может войти в сговор с нарушителем.

По оценкам западных экспертов до 80% рынка биометрии сегодня занимают устройства идентификации по отпечаткам пальцев. Это объясняется следующим: во-первых, это один самых доступных и недорогих методов, во-вторых, методика идентификации по отпечаткам пальцев проста в использовании, удобна и лишена психологических барьеров, которые имеются, например, у систем, требующих воздействия на глаз световым пучком.

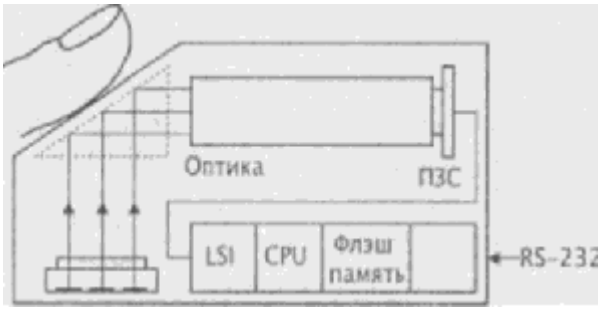
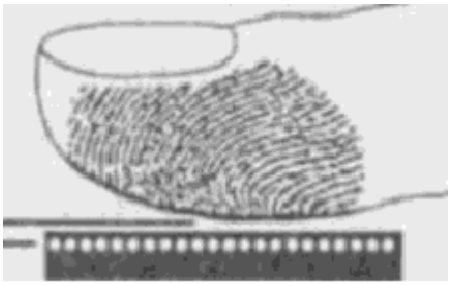


Рис. 3. Функциональная схема системы FIU фирмы SONY

Свет, падающий на призму, отражается от поверхности, соприкасаемой с пальцем пользователя, и выходит через другую сторону призмы, попадая на оптический сенсор (обычно, монохромная видеокамера на основе ПЗС-матрицы), где формируется изображение. Недостатки такой системы: отражение сильно зависит от параметров кожи - сухости, присутствия масла, бензина, других химических

элементов. Например, у людей с сухой кожей наблюдается эффект размытия изображения и в результате - высокая доля ложных срабатываний.



Другой способ использует методику измерения электрического поля пальца с использованием полупроводниковой пластины. Когда пользователь устанавливает палец в сенсор, он выступает в качестве одной из пластин конденсатора (рис. 4). Другая пластина конденсатора - это поверхность сенсора, которая состоит из кремниевого чипа, содержащего 90 тыс. конденсаторных пластин с шагом считывания 500 точек на дюйм. В результате получается 8-битовое растровое изображение гребней и впадин пальца.

Естественно, в данном случае жировой баланс кожи и степень чистоты рук пользователя не играет никакой роли. Система идентификации в этом случае, получается гораздо более компактная. Недостатки метода - кремниевый чип требует эксплуатации в герметичной оболочке, а дополнительные покрытия уменьшают чувствительность системы. Кроме того, некоторое влияние на изображение может оказать сильное внешнее электромагнитное излучение.

Существует еще один метод реализации таких систем. Его разработала компания «Who Vision Systems». В основе их системы TactileSense - электрооптический полимер. Этот материал чувствителен к разности электрического поля между гребнями и впадинами кожи. Градиент электрического поля конвертируется в оптическое изображение высокого разрешения, которое затем переводится в цифровой формат, который уже можно передавать в ПК по параллельному порту или USB-интерфейсу. Метод также нечувствителен к состоянию кожу и степени ее загрязнения, в том числе и химического. Вместе с тем считывающее устройство имеет миниатюрные размеры и может быть встроено, например, в компьютерную клавиатуру. По утверждению производителей, система имеет колоссально низкую себестоимость (на уровне нескольких десятков долларов).

2.2 Идентификация по радужной оболочке глаз

Первооткрывателем в области идентификации личности по радужной оболочке глаза является доктор Джон Даугман. В 1994 г. он запатентовал в США метод распознавания радужной оболочки глаза (US Patent S, 291, 560). Разработанные им алгоритмы используются до сих пор.

С помощью этих алгоритмов необработанные видеоизображения глаза преобразуются в уникальный идентификационный двоичный поток Iris-код, полученный в результате определения позиции радужки, ее границы и выполнения других математических операций для описания текстуры радужки в виде последовательности чередования фаз, похожей на штрих-код.

Полученный таким образом Iris-код используется для поиска совпадений в базах данных (скорость поиска - около 1 млн. сравнения Iris-кодов в 1 с) и для подтверждения или неподтверждения заявленной личности

Преимущество сканеров для радужной оболочки глаза состоит в том, что они не требуют от пользователя сосредоточения на цели, так как образец пятен на радужной оболочке находится на поверхности глаза. Фактически видеоизображение глаза может быть отсканировано на расстоянии менее 1 м, что делает возможным использование сканеров для радужной оболочки глаза, допустим, в банкоматах. Разработкой технологии идентификации личности на основе принципа сканирования радужной оболочки глаза в настоящее время занимаются более 20 компаний, в том числе British Telecom, Sensar, японская компания Oki.

Различают активные и пассивные системы распознавания. В системах первого типа пользователь должен сам настроить камеру, передвигая ее для более точной наводки. Пассивные системы проще в использовании, поскольку камера в них настраивается автоматически. Высокая надежность этого оборудования позволяет применять его даже в исправительных учреждениях.

В качестве примера современной системы идентификации на основе анализа радужной оболочки глаза рассмотрим решение, предложенное компанией LG.

Система IrisAccess позволяет менее чем за 1 с отсканировать рисунок радужной оболочки глаза, обработать и сравнить с 4 тыс. других записей, которые она хранит в своей памяти, а затем послать соответствующий сигнал в охранную

систему. Технология - полностью бесконтактная. На основе изображения радужной оболочки глаза строится компактный цифровой код размером 512 байт. Устройство имеет высокую надежность по сравнению с большинством известных систем биометрического контроля, поддерживает объемную базу данных, выдает звуковые инструкции на русском языке, позволяет интегрировать в систему карты доступа и ПИН-клавиатуры. Один контроллер поддерживает четыре считывателя Система может быть интегрирована с LAN Система IrisAccess 3000 состоит из оптического устройства внесения в реестр E01J3000, удаленного оптического устройства R01J3000, контрольного устройства опознавания ICLI3000, платы захвата изображения, дверной интерфейсной платы и PC-сервера. Если требуется осуществлять контроль за несколькими входами, то ряд удаленных устройств, включая ICU3000 и R01J3000, может быть подключен к PC-серверу через локальную сеть (LAN).

Представляет интерес камера для идентификации личности путем сканирования радужной оболочки глаза, используемая в системах защиты и безопасности для компьютеров типа десктоп/лэптоп. Разработки визуальных систем (Vision Systems) компании Panasonic и хорошо показавшие себя на прак-тике разработки в области идентификации личности на основе рисунка радужной оболочки глаз компании Iridian Technologies позволили создать легкие в использовании и отличающиеся высокой точностью средства, которые можно использовать в широком диапазоне современных и будущих потребностей в области обеспечения безопасности.

Камера Authenticam™ компании Panasonic в сочетании с программным продуктом PrivateID™ компании Indian Technologies представляет собой экономически выгодный и надежный путь обеспечения безопасности доступа. Для такой камеры характерны безопасность и простота использования. Достаточно взглянуть в объектив камеры с расстояния приблизительно 50 см, и менее чем через 2 с произойдет захват изображения.

Программный продукт PrivateID™ обрабатывает рисунок радужной оболочки глаз и кодирует полученную информацию в виде 512-байтовой записи IrisCode. Эти записи вводятся для хранения в память и используются для сравнения с другими записями кодов IrisCodes - для идентификации личности при любых транзакциях и деловых операциях, когда для сравнения представляется радужная оболочка глаза живого человека.

Дифференциатор ключей для идентификации личности по рисунку радужной оболочки глаза осуществляет поиск в базе данных для нахождения

соответствующего идентификационного кода. При этом база данных может состоять из неограниченного числа записей кодов IrisCode. Технология допуска, основанная на сканировании радужной оболочки глаза, уже несколько лет успешно применяется в государственных организациях США и в учреждениях с высокой степенью секретности (в частности, на заводах по производству ядерного вооружения). Эффективность этого способа доказана, он безопасен для пользователя и надежен в работе. Он обеспечивает моментальную аутентификацию личности, предназначенную для замены символов ПИН-кодов и паролей.

Многие эксперты подчеркивают «незрелость» технологии, хотя потенциальные возможности метода достаточно высоки, так как характеристики рисунка радужной оболочки человеческого глаза достаточно стабильны и не изменяются практически в течение всей жизни человека, невосприимчивы к загрязнению и ранам. Отметим также, что радужки правого и левого глаза по рисунку существенно различаются. Этот метод идентификации отличается от других большей сложностью в использовании, более высокой стоимостью аппаратуры и жесткими условиями регистрации.

2.3 Идентификация по капиллярам сетчатки глаз

При идентификации по сетчатке глаза измеряется угловое распределение кровеносных сосудов на поверхности сетчатки относительно слепого пятна глаза и другие признаки. Капиллярный рисунок сетчатки глаз различается даже у близнецов и может

быть с большим успехом использован для идентификации личности. Всего насчитывают около 250 признаков. Такие биометрические терминалы обеспечивают высокую достоверность идентификации, сопоставимую с дактилоскопией, но требуют от проверяемого лица фиксации взгляда на объективе сканера.

Сканирование сетчатки происходит с использованием инфракрасного света низкой интенсивности, направленного через зрачок к кровеносным сосудам на задней стенке глаза. Сканеры сетчатки глаза получили широкое распространение в СКУД особо секретных объектов, так как у них один из самых низких процентов отказа в доступе зарегистрированных пользователей и практически не бывает ошибочного

разрешения доступа. Однако изображение радужной оболочки должно быть четким, поэтому катаракта может отрицательно воздействовать на качество идентификации личности.

Начало разработок этого направления идентификации относится к 1976 г., когда в США была образована компания Eye Dentify, которая до настоящего времени сохраняет монополию на производство коммерческих систем аутентификации по ретине.

Основным устройством для системы такого типа является бинокулярный объектив. При осуществлении процедуры аутентификации пользователь должен прильнуть глазами к окулярам и, глядя вовнутрь, сфокусировать взгляд на изображении красного цвета. Затем ему следует дождаться смены цвета на зеленый (что укажет на правильную фокусировку) и нажать на стартовую кнопку. Сканирование глазного дна выполняется источником инфракрасного излучения, безопасного для глаз. Достаточно смотреть в глазок камеры менее минуты. За это время система успевает подсветить сетчатку и получить отраженный сигнал. Для сканирования сетчатки используется инфракрасное излучение низкой интенсивности, направленное через зрачок к кровеносным сосудам на задней стенке глаза. Отраженное от ретины излучение фиксируется специальной чувствительной камерой.

Замеры ведутся по 320 точкам фотодатчиками и результирующий аналоговый сигнал с помощью микропроцессора преобразуется в цифровой вид. При этом используется алгоритм быстрого преобразования Фурье. Полученный цифровой вектор, состоящий из коэффициентов Фурье, сравнивается с зарегистрированным эталоном, хранящимся в памяти системы. Благодаря такому методу преобразования и представления изображения глазного дна для хранения каждого эталона расходуется по 40 байт. Память терминала Eye Dentification System 7.5, реализующего этот алгоритм, рассчитана на запоминание до 1200 эталонов. Время регистрации составляет примерно 30 с, время аутентификации - 1,5 с. Коэффициент ошибок 1-го рода - 0,01 %, 2-го рода - 0,0001 % (т. е. вероятность ошибок 1-го рода - 0,0001, 2-го рода - 0,000001).

С точки зрения безопасности данная система выгодно отличается от всех других, использующих биометрические терминалы, не только малым значением коэффициентов ошибок как l-ro, так и 2-го рода, но и использованием специфического аутентификациоиного атрибута, который практически невозможно негласно подменить для обмана системы при проверке.

К недостаткам подобных систем следует отнести психологический фактор: не всякий человек отважится посмотреть в неведомое темное отверстие, где что-то светит в глаз. К тому же надо следить за положением глаза относительно отверстия, поскольку подобные системы, как правило, чувствительны к неправильной ориентации сетчатки. Сканеры для сетчатки глаза получат большое распространение при организации доступа к сверхсекретным системам, поскольку гарантируют один из самых низких процентов отказа в доступе зарегистрированных пользователей и почти нулевой процент ошибок.

2.4 Идентификация по геометрии и тепловому изображению лица

Идентификация человека но чертам (геометрии) лица - одно из самых динамично развивающихся направлений в биометрической индустрии. Привлекательность данного метода основана на том, что он наиболее близок к тому, как люди обычно идентифицируют друг друга. Рост мультимедийных технологий, благодаря которым можно увидеть все больше видеокамер, установленных на городских улицах и площадях, аэропортах, вокзалах и других местах скопления людей, определили развитие этого направления.

Техническая реализация метода - более сложная (с математической точки зрения) задача, чем распознавание отпечатков пальцев, и, кроме того, требует более дорогостоящей аппаратуры (нужна цифровая видео- или фотокамера и плата захвата видеоизображения). У этого метода есть один существенный плюс: для хранения данных об одном образце идентификационного шаблона требуется совсем немного памяти, так как человеческое лицо можно «разобрать» на относительно небольшое количество участков, неизменных у всех людей. Например, для вычисления уникального шаблона, соответствующего конкретному человеку, требуется всего от 12 до 40 характерных участков.

Обычно камера устанавливается на расстоянии нескольких десятков сантиметров от объекта. Получив изображение, система анализирует различные параметры лица (например, расстояние между глазами и носом). Большинство алгоритмов позволяет компенсировать наличие у исследуемого индивида очков, шляпы и бороды. Для этой цели обычно используется сканирование лица в инфракрасном диапазоне, но пока системы такого типа не дают устойчивых и очень точных

результатов.

Распознавание человека по изображению лица выделяется среди биометрических систем тем, что, во-первых, не требует специального дорогостоящего оборудования. Для большинства приложений достаточно только персонального компьютера и обычной видеокамеры. Во-вторых, отсутствует физический контакт человека с устройствами. Не надо ни к чему прикасаться или специально останавливаться и ждать срабатывания системы. В большинстве случаев достаточно просто пройти мимо или задержаться перед камерой на несколько секунд. Распознавание изображений аналогично распознаванию образов.

Такие задачи не имеют точного аналитического решения. При этом требуется выделение ключевых признаков, характеризующих зрительный образ, определение относительной важности признаков путем выбора их весовых коэффициентов и учет взаимосвязей между признаками.

Компания ISS разработала ряд алгоритмов, позволяющих обрабатывать видеоданные в режиме реального времени и производить локализацию, определять положение головы и отслеживать перемещение с целью дальнейшего распознавания.

В настоящее время существует четыре основных метода распознавания лица, различающихся сложностью реализации и целью применения :

- «eigenfaces»;

- анализ «отличительных черт»;

- анализ на основе «нейронных сетей»;

- метод «автоматической обработки изображения лица».

«Eigenface» можно перевести как «собственное лицо». Эта технология использует двумерные изображения в градациях серого, которые представляют отличительные характеристики изображения лица. Метод «eigenface» часто используется в качестве основы для других методов распознавания лица. Комбинируя характеристики 100-120 «eigenface», можно восстановить большое число лиц. В момент регистрации «eigenface» каждого конкретного человека представляется в виде ряда коэффициентов. Для режима установления подлинности, в котором изображение используется для проверки идентичности, «живой» шаблон сравнивается с уже зарегистрированным шаблоном с целью

определения коэффициента различия. Степень различия между шаблонами определяет факт идентификации. Технология «eigenface» оптимальна при использовании в хорошо освещенных помещениях, когда есть возможность сканирования лица в фас.

Метод анализа «отличительных черт» **-** наиболее широко используемая технология идентификации. Она подобна методу «Eigenface», но в большей степени адаптирована к изменению внешности или мимики человека (улыбающееся или хмурящееся лицо). В технологии «отличительных черт» используются десятки характерных особенностей различных областей лица, причем с учетом их относительного местоположения. Индивидуальная комбинация этих параметров определяет особенности каждого конкретного лица. Лицо человека уникально, но достаточно динамично, так как человек может улыбаться, отпускать бороду и усы, надевать очки - все это увеличивает сложность процедуры идентификации. Например, при улыбке наблюдается некоторое смещение частей лица, расположенных около рта, что в свою очередь будет вызывать подобное движение смежных частей. Учитывая такие смещения, можно однозначно идентифицировать человека и при различных мимических изменениях лица. Так как этот анализ рассматривает локальные участки лица, допустимые отклонения могут находиться в пределах до 25° в горизонтальной плоскости, и приблизительно до 15° в вертикальной плоскости и требует достаточно мощной и дорогой аппаратуры, что соответственно снижает возможности распространения данного метода.

В методе, основанном на нейронной сети, характерные особенности обоих лиц - зарегистрированного и проверяемого сравниваются на совпадение. «Нейронные сети» используют алгоритм, устанавливающий соответствие уникальных параметров лица проверяемого человека и параметров шаблона, находящегося в базе данных, при этом применяется максимально возможное число параметров. По мере сравнения определяются несоответствия между лицом проверяемого и шаблона из базы данных, затем запускается механизм, который с помощью соответствующих весовых коэффициентов определяет степень соответствия проверяемого лица шаблону из базы данных. Этот метод увеличивает качество идентификации лица в сложных условиях.

Метод автоматической обработки изображения лица - наиболее простая технология, использующая расстояния и отношение расстояний между легко определяемыми точками лица, такими, как глаза, конец носа, уголки рта. Хотя данный метод не столь мощный, как «eigenfaces» или «нейронная сеть», он может быть достаточно эффективно использован в условиях слабой освещенности.

Задачу идентификации личности человека по видеоизображению можно разбить на несколько этапов.

Локализация лица в кадре.

Для локализации лица в кадре разработан алгоритм на основе нейронной сети, который сканирует исходное изображение в разных масштабах, оценивая по ключевым признакам каждый участок изображения с определенной вероятностью, и классифицирует, является ли данный участок лицом или нет. Выделение ключевых признаков осуществляется путем автоматического анализа достаточно большой обучающей выборки, охватывающей большинство возможных ситуаций (например, изменение внешности, условий освещенности, ракурса и т. п.).

Определение положения головы.

Определение положения головы человека является важным этапом и позволяет внести поправки при дальнейшем распознавании. На этом этапе созданная компанией трехмерная модель головы сопоставляется с изображением головы в кадре. При этом оцениваются такие параметры, как угол поворота головы по осям X, Y, Z, точный замер и смещение изображения в кадре.

Отслеживание перемещения лица от кадра к кадру.

При идентификации движущегося в поле зрения камеры человека необходимо отслеживать перемещение лица от кадра к кадру. Имея несколько изображений одного и того же человека в разных ракурсах, программа выбирает наиболее удачный с ее точки зрения кадр и сохраняет его в базе данных. Обрабатывая несколько изображений одного и того же человека в разных ракурсах, можно добиться очень высокой точности распознавания.

Сравнение изображения с данными базы.

В настоящее время компания ISS ведет разработки алгоритма сравнения лица с имеющимся в базе данных. Этот этап является логическим завершением в цепочке алгоритма идентификации личности по видеоизображению.

2.5 Идентификация но геометрии кисти руки

Метод идентификации пользователей по геометрии руки по своей технологической структуре и уровню надежности вполне сопоставим с методом идентификации личности по отпечатку пальца. Статистическая вероятность существования двух кистей рук с одинаковой геометрией чрезвычайно мала. Но признаки руки меняются с возрастом, а само устройство имеет сравнительно большие размеры.

Математическая модель идентификации по данному параметру требует немного информации - всего 9 байт, что позволяет хранить большой объем записей и быстро осуществлять поиск. Устройства идентификации личности по геометрии руки находят широкое применение. Так, в США устройства для считывания отпечатков ладоней в настоящее время установлены более чем на 8000 объектах. Наиболее популярное устройство Handkey сканирует как внутреннюю, так и боковую сторону ладони, используя для этого встроенную видеокамеру и алгоритмы сжатия. При этом оценивается более 90 различных характеристик, включая размеры самой ладони (три измерения), длину и ширину пальцев, очертания суставов и т. п. Устройства, которые могут сканировать и другие параметры руки, в настоящее время разрабатываются несколькими компаниями, в том числе BioMet Partners, Palmetrics и BTG.

Представителем этого направления разработок СКУД является американская компания Steller Systems, выпускающая терминал Identimat. Для считывания геометрических характеристик кисти ее кладут ладонью вниз на специальную панель. Через прорези в ее поверхности оптические сенсорные ячейки сканируют четыре кольца. Эти ячейки определяют стартовые точки по двум парам пальцев - указательному и среднему, безымянному и мизинцу. Каждый палец сканируется по всей длине, при этом замеряется длина, изгиб и расстояние до «соседа». Если каждое измерение укладывается в определенные допустимые рамки зарегистрированного эталонного набора данных, то результат аутентификации будет для пользователя положительным. Цифровой эталон хранится либо в базе данных, либо в памяти идентификационной карточки. При этом с целью обеспечения защиты данные шифруются.

Рассматриваемый терминал прост в обращении и надежен. Время обработки - всего 1 с; время регистрации - 1,5 мин; вероятность ошибок 1-го рода- 0,01, 2-го рода - 0,015 (т.е. коэффициенты 1 и 1,5% соответственно). Для хранения эталона используется 17 байт памяти.

Отличительной особенностью алгоритма работы этого терминала является наличие так называемых битов качества, которые регулируют рамки допустимых

отклонений в зависимости от качества изображения кисти. Однако настораживает тот факт, что у каждого сотого сотрудника могут появиться проблемы с проходом на рабочее место. И каждый стопятидесятый может оказаться чужим.

На базе подобной технологии биометрии японская фирма Mitsubishi Electric построила контрольно-пропускной терминал автономного типа Palm Recognition System. Его отличие от американского прототипа состоит в том, что производится считывание геометрических размеров силуэта кисти руки со сжатыми пальцами, в то время как у американцев пальцы для измерения должны представляться растопыренными. Благодаря такому подходу на результатах оценки биометрических характеристик в японской системе не сказывается появление на ладони ран или грязи. Однако вероятность ошибок 1-го рода также составляет 0,01, но ошибок 2-го рода - 0,000001. Время обработки занимает 2 с, время регистрации при оформлении допуска - 20 с. Память системы позволяет хранить до 220 эталонов.

В настоящее время идентификация пользователей по геометрии руки используется в законодательных органах, международных аэропортах, больницах, иммиграционных службах и т. д. Достоинства идентификации по геометрии ладони сравнимы с достоинствами идентификации по отпечатку пальца с точки зрения надежности, хотя устройство для считывания отпечатков ладоней занимает больше места.

3. Особенности реализации динамических методов биометрического контроля

3.1 Идентификация по почерку и динамике подписи

Основой аутентификации личности по почерку и динамике написания контрольных фраз (подписи) является уникальность и стабильность динамики этого процесса для каждого человека, характеристики которой могут быть измерены, переведены в цифровой вид и подвергнуты компьютерной обработке. Таким образом, при

аутентификации для сравнения выбирается не продукт письма, а сам процесс.

Разработка аутентификационных автоматов на базе анализа почерка (подписи - как варианта объекта исследования), предназначенных для реализации контрольно-пропускной функции, была начата еще в начале 1970-х г. В настоящее время на рынке представлено несколько эффективных терминалов такого типа.

Подпись - такой же уникальный атрибут человека, как и его физиологические характеристики. Кроме того, это и более привычный для любого человека метод идентификации, поскольку он, в отличие от снятия отпечатков пальцев, не ассоциируется с криминальной сферой. Одна из перспективных технологий аутентификации основана на уникальности биометрических характеристик движения человеческой руки во время письма. Обычно выделяют два способа обработки данных о подписи: простое сравнение с образцом и динамическую верификацию. Первый весьма ненадежен, так как основан на обычном сравнении введенной подписи с хранящимися в базе данных графическими образцами. Из-за того, что подпись не может быть всегда одинаковой, этот метод дает большой процент ошибок. Способ динамической верификации требует намного более сложных вычислений и позволяет в реальном времени фиксировать параметры процесса подписи, такие, как скорость движения руки на разных участках, сила давления и длительность различных этапов подписи. Это дает гарантии того, что подпись не сможет подделать даже опытный графолог, поскольку никто не в состоянии в точности скопировать поведение руки владельца подписи. Пользователь, используя стандартный дигитайзер и ручку, имитирует свою обычную подпись, а система считывает параметры движения и сверяет их с теми, что были заранее введены в базу данных. При совпадении образа подписи с эталоном система прикрепляет к подписываемому документу информацию, включающую имя пользователя, адрес его электронной почты, должность, текущее время и дату, параметры подписи, содержащие несколько десятков характеристик динамики движения (направление, скорость, ускорение) и другие. Эти данные шифруются, затем для них вычисляется контрольная сумма, и далее все это шифруется еще раз, образуя так называемую биометрическую метку. Для настройки системы вновь зарегистрированный пользователь от пяти до десяти раз выполняет процедуру подписания документа, что позволяет получить усредненные показатели и доверительный интервал. Впервые данную технологию использовала компания РепОр.

Идентификацию по подписи нельзя использовать повсюду, в частности, этот метод не подходит для ограничения доступа в помещения или для доступа в

компьютерные сети. Однако в некоторых областях, например в банковской сфере, а также всюду, где происходит оформление важных документов, проверка правильности подписи может стать наиболее эффективным, а главное, необременительным и незаметным способом. До сих пор финансовое сообщество не спешило принимать автоматизированные методы идентификации подписи для кредитных карточек и проверки заявления, потому что подписи все еще слишком легко подделать. Это препятствует внедрению идентификации личности по подписи в высокотехнологичные системы безопасности.

Устройства идентификации по динамике подписи используют геометрические или динамические признаки рукописного воспроизведения подписи в реальном масштабе времени. Подпись выполняется пользователем на специальной сенсорной панели, с помощью которой осуществляется преобразование изменений приложенного усилия нажатия на перо (скорости, ускорения) в электрический аналоговый сигнал. Электронная схема преобразует этот сигнал в цифровой вид, приспособленный для машинной обработки. При формировании «эталона» необходимо учитывать, что для одного и того же человека характерен некоторый разброс характеристик почерка от одного акта к другому. Чтобы определить эти флуктуации и назначить рамки, пользователь при регистрации выписывает свою подпись несколько раз. В результате формируется некая «стандартная модель» (сигнатурный эталон) для каждого пользователя, которая записывается в память системы.

В качестве примера реализации такого метода идентификации можно рассматривать систему Automatic Personal Verification System, разработанную американской корпорацией NCR Corp. Эта система на испытаниях продемонстрировала следующие результаты: коэффициент ошибок 1-го рода - 0,015%, 2-го рода - 0,012% (в случае, если злоумышленник не наблюдал процесс исполнения подписи законным пользователем) и 0,25 % (если он наблюдал).

Системы аутентификации по почерку поставляются на рынок, например, фирмами Inforete и De La Rue Systems (США), Thompson T1TN (Франция) и рядом других. Английская фирма Quest Micropad Ltd выпустила устройство QSign, особенностью которого является то, что сигнатурный эталон может храниться как в памяти системы, так и в памяти идентификационной карточки пользователя. Пороговое значение коэффициентов ошибок может изменяться в зависимости от требуемой степени безопасности. Подпись выполняется обычной шариковой ручкой или карандашом на специальной сенсорной панели, входящей в состав терминала.

Основное достоинство подписи по сравнению с использованием, например, дактилоскопии в том, что это распространенный и общепризнанный способ подтверждения своей личности (например, при получении банковских вкладов). Этот способ не вызывает «технологического дискомфорта», как бывает в случае снятия отпечатков пальцев, что ассоциируется с деятельностью правоохранительных органов. В то же время подделка динамики подписи - дело очень трудновыполнимое (в отличие, скажем, от воспроизведения рисунка подписи). Причем благодаря росписи не на бумаге, а на сенсорной панели, значительно затрудняется копирование злоумышленником ее начертания.

Идентификация по ритму работы на клавиатуре основана на измерении временных интервалов между двумя последовательными ударами по клавишам при печатании знаков.

3.2 Идентификация но голосу и особенностям речи

Биометрический подход, связанный с идентификацией голоса, удобен в применении. Однако основным и определяющим недостатком этого подхода является низкая точность идентификации. Например, человек с простудой или ларингитом может испытывать трудности при использовании данных систем. Причинами внедрения этих систем являются повсеместное распространение телефонных сетей и практика встраивания микрофонов в компьютеры и периферийные устройства. В качестве недостатков таких систем можно назвать факторы, влияющие на результаты распознавания: помехи в микрофонах, влияние окружающей обстановки на результаты распознавания (шум), ошибки при произнесении, различное эмоциональное состояние проверяемого в момент регистрации эталона и при каждой идентификации, использование разных устройств регистрации при записи эталонов и идентификации, помехи в низкокачественных каналах передачи данных и т. п.

При рассмотрении проблемы аутентификации по голосу важными вопросами с точки зрения безопасности являются следующие:

- Как бороться против использования магнитофонных записей парольных фраз, перехваченных во время установления контакта законного пользователя с аутентификационным терминалом?

- Как защитить систему от злоумышленников, обладающих способностью к имитации голоса, если им удастся узнать парольную фразу?

Ответом на первый вопрос является генерация системой псевдослучайных паролей, которые повторяются вслед за ней пользователем, а также применение комбинированных методов проверки (дополняя вводом идентификационной карточки или цифрового персонального кода).

Ответ на второй вопрос не так однозначен. Человек вырабатывает свое мнение о специфике воспринимаемого голоса путем оценки некоторых его характерных качеств, не обращая внимание при этом на количественную сторону разнообразных мелких компонент речевого сигнала. Автомат же наоборот, не обладая способностью улавливать обобщенную характеристику голоса, свой вывод делает, основываясь на конкретных параметрах речевого сигнала и производя их точный количественный анализ.

Специфическое слуховое восприятие человека приводит к тому, что безупречное воспроизведение профессиональными имитаторами голосов возможно лишь тогда, когда подражаемый субъект характеризуется ярко выраженными особенностями произношения (интонационной картиной, акцентом, темпом речи и т. д.) или тембра (гнусавостью, шепелявостью, картавостью и т. д.). Именно этим следует объяснить тот факт, что даже профессиональные имитаторы оказываются не в состоянии подражать ординарным, не примечательным голосам.

В противоположность людям распознающие автоматы, свободные от субъективного отношения к воспринимаемым образам, производят аутентификацию (распознавание) голосов объективно, на основе строго детерминированных и априори заданных признаков. Обладая «нечеловеческим» критерием оценки схожести голосов, системы воспринимают голос человека через призму своих признаков. Вследствие этого, чем сложнее и «непонятнее» будет совокупность признаков, по которым автомат распознает голос, тем меньше будет вероятность его обмана. В гоже время, несмотря на то, что проблема имитации очень важна и актуальна с практической точки зрения, она все же далека от окончательного решения. Прежде всего до конца не ясен ответ на вопрос, какие именно параметры речевого сигнала наиболее доступны подражанию и какие из них наиболее трудно поддаются ему.

Выбор параметров речевого сигнала способных наилучшим образом описать индивидуальность голоса является, пожалуй, самым важным этапом при

построении систем автоматической аутентификации по голосу. Такие параметры сигнала, называемые признаками индивидуальности, помимо эффективности представления информации об особенностях голоса диктора, должны обладать рядом других свойств. Во-первых, они должны быть легко измеряемы и мало зависеть от мешающих факторов окружающей среды (шумов и помех). Во-вторых, они должны быть стабильными во времени. В-третьих, не должны поддаваться имитации.

Постоянно ведутся работы по повышению эффективности систем идентификации по голосу. Известны системы аутентификации по голосу, где применяется метод совместного анализа голоса и мимики, ибо, как оказалось, мимика говорящего характерна только ему и будет отличаться от говорящего те же слова мимики другого человека.

Разрабатываются комбинированные системы, состоящие из блоков идентификации и верификации голоса. При решении задачи идентификации находится ближайший голос (или несколько голосов) 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.

В последнее время ведутся активные разработки по усовершенствованию и модификации голосовых систем идентификации личности, поиск новых подходов для характеристики человеческой речи, комбинации физиологических и поведенческих факторов.

Задача повышения надежности распознавания может быть решена за счет привлечения грамматической и семантической информации в системах распознавания речи. Для решения этой задачи разработана (при участии экспертов: лингвистов, рядовых носителей языка) модель входного языка, учитывающая особенности их грамматического и семантического поведения (28 основных грамматических классов, около 300 грамматических разрядов слов), ее компьютерное воплощение - лингвистическая база знаний (ЛБЗ) и лингвистический процессор (ЛП). В состав ЛБЗ входят: обширный грамматический словарь - объемом около 100000 единиц; словари словосочетаний; словари униграмм и лексических биграмм; грамматические таблицы и словарь моделей управления. Программы синтактико-семантического анализа, входящие в состав ЛП, обеспечивают: быстрое отсеивание маловероятных вариантов распознавания (локальный анализ), учет обнаруженных при анализе грамматических событий, характеризующих

регулярность грамматической структуры и степень грамматичности предложения в целом или отдельных групп (и тем самым возможность выбора в качестве окончательного результата распознавания неграмматичных, но допустимых в речи вариантов). Для решения многокритериальной задачи выбора окончательного варианта были разработаны специальные эвристики метауровня. Лингвистический модуль (ЛБЗ и ЛП) позволяет повысить надежность акустического и фонетического распознавания с 94-95 до 95-97 %.

Уделяется внимание проблемам автоматизированного формирования и сопровождения ЛБЗ систем распознавания речи (для английского и русского языков): построение тезауруса, коррекция словаря лексических n-грамм на основе синтактико-семантической информации и др. Новые методы, как показывают результаты экспериментов, позволяют повысить надежность распознавания еще на 1 %.

Сегодня идентификация по голосу используется для управления доступом в помещения средней степени секретности, например, лаборатории производственных компаний. Лидерами в разработке таких систем являются компании T-Netix, ITT Nuance, Veritel. В системе фирмы Texas Instruments (TI) парольные фразы состояли из 4-словного предложения, причем каждое слово было односложным. Каждая фраза являлась 84 байтами информации. Время аутентификации составляло 5,3 с. Для предотвращения использования заранее записанного на магнитофон пароля система генерировала слова в произвольной последовательности. Общее время проверки на КПП составляло 15 с на одного человека. Для четырех парольных фраз ошибка 1-го рода составила 0,3 %, 2-го рода - 1 %.

3.3 Идентификация по ритму работы на клавиатуре

Современные исследования показывают, что клавиатурный почерк пользователя обладает некоторой стабильностью, что позволяет достаточно однозначно идентифицировать пользователя. Применяются статистические методы обработки исходных данных и формирования выходного вектора, являющегося идентификатором данного пользователя. В качестве исходных данных используют временные интервалы между нажатием клавиш на клавиатуре и время их

удержания. При этом временные интервалы между нажатием клавиш характеризуют темп работы, а время удержания клавиш характеризует стиль работы с клавиатурой - резкий удар или плавное нажатие.

Идентификация пользователя по клавиатурному почерку возможна следующими способами:

- по набору ключевой фразы;

- по набору произвольного текста.

Принципиальное отличие этих двух способов заключается в том, что в первом случае используется ключевая фраза, задаваемая пользователем в момент регистрации его в системе (пароль), а во втором случае используются ключевые фразы, генерируемые системой каждый раз в момент идентификации пользователя. Подразумеваются 2 режима работы:

- обучение;

- идентификация.

На этапе обучения пользователь вводит некоторое число раз предлагаемые ему тестовые фразы При этом рассчитываются и запоминаются эталонные характеристики данного пользователя. На этапе идентификации рассчитанные оценки сравниваются с эталонными, на основании чего делается вывод о совпадении или несовпадении параметров клавиатурного почерка. Выбор текста, на котором выполняется обучение системы, - достаточно важный этап для нормального функционирования системы. Предлагаемые пользователю фразы необходимо подбирать таким образом, чтобы используемые в них символы полностью и равномерно покрывали рабочее поле клавиатуры. Более того, если в процессе обучения системы видно, что статистические характеристики отдельных клавиш имеют существенный разброс, необходимо формировать очередную тестовую фразу таким образом, чтобы уменьшить эту неопределенность. Возможна организация «неявного» процесса обучения системы, когда программа перехватывает весь ввод с клавиатуры и соответственно рассчитывает эталонные характеристики пользователя. Данная процедура достаточно легко организуется практически в любой операционной системе. В DOS для этого используется перехват прерываний от клавиатуры, в Windows - стандартный механизм ловушек (hooks).

Однако существует ряд ограничений по применению данного способа на практике. Применение способа идентификации по клавиатурному почерку целесообразно только по отношению к пользователям с достаточно длительным опытом работы с компьютером и сформировавшимся почерком работы на клавиатуре, т. е. к программистам, секретарям и т. д. В противном случае вероятность неправильного опознания «легального» пользователя существенно возрастает и делает непригодным данный способ идентификации на практике. Исходя из теории машинописи и делопроизводства можно определить время становления почерка работы с клавиатурой, при котором достигается необходимая вероятность идентификации пользователя: примерно 6 месяцев.

Заключение

В заключение хочется отметить, что обойтись без биометрической идентификации, если необходимо получить позитивные, надежные и неопровержимые результаты проверки, невозможно. Ожидается, что в самом ближайшем будущем пароли и ПИН-коды уступят место новым, более надежным средствам авторизации и аутентификации.

Литература

Тихонов В А., Райх В. В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: Уч. пособие. М.: Гелиос АРВ, 2006.

Абалмазов Э. И. Энциклопедия безопасности. Справочник каталог, 1997.

Тарасов Ю Контрольно-пропускной режим на предприятии. Защита информации // Конфидент, 2002. № 1. С. 55-61.

Сабынин В. Н. Организация пропускного режима первый шаг к обеспечению безопасности и конфиденциальности информации // Информост -радиоэлектроники и телекоммуникации, 2001. № 3 (16).

Татарченко И. В., Соловьев Д. С. Концепция интеграции унифицированных систем безопасности // Системы безопасности. № 1 (73). С. 86-89.

Мащенов Р. Г. Системы охранной сигнализации: основы теории и принципы построения: учебное пособие. М.: Горячая линия - Телеком, 2004

Горлицин И. Контроль и управление доступом - просто и надежно КТЦ «Охранные системы», 2002.

Барсуков В. С. Интегральная защита информации // Системы безопасности, 2002. №5, 6.

Стасенко Л. СКУД - система контроля и управления доступом // Все о вашей безопасности. Группа компаний «Релвест» (Sleo@relvest).

Абрамов А. М., Никулин О. Ю, Петрушин А. И. Системы управления доступом. М.: «Оберег-РБ», 1998.

Предтеченский В И , Рыжухин Д. В , Сергеев М. С. Анализ возможности использования кодонаборных устройств (клавиатур) в системах контроля и управления доступом высокого уровня безопасности. М.: МГИФИ, 2005.

Гинце А. Новые технологии в СКУД // Системы безопасности, 2005.

Злотник Е. Touch Memory - новый электронный идентификатор // Монитор, 1994. №6 С. 26-31.

Филипп Х. Уокер Электронные системы охраны. Наилучшие способы предотвращения преступлений / Пер. с англ. М.: «За и против», 1991

Флорен М. В. Организация управления доступом // Защита информации «Конфидент», 1995. № 5. С. 87-93.

Барсуков В. С. Биоключ - путь к безопасности // Специальная техника,

Крахмалев А. К. Средства и системы контроля и управления доступом. Учебное пособие. М.: НИЦ «Охрана» ГУВО МВД России. 2003.

Мальцев И. В. Системы контроля доступом // Системы безопасности,1996. № 1. С. 43-45.

Комплексные системы безопасности. Каталог. М.: Научно-производственный центр «Нелк», 2001.