

МЕТОДЫ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ ДЛЯ ИСПОЛЬЗОВАНИЯ В ПАСПОРТНОЙ СИСТЕМЕ

И.Д. ГОРБЕНКО, И.В. ОЛЕШКО

В работе рассматриваются методы биометрической аутентификации. Приводятся критерии оценки биометрических систем. Даются рекомендации по использованию биометрических методов в паспортной системе.

Ключевые слова: биометрический паспорт, биометрическая идентификация, статическая биометрия, динамическая биометрия, коэффициент равной вероятности ошибок, биометрическая система аутентификации.

ВВЕДЕНИЕ

В Украине и в странах ЕС ведется активная работа по внедрению биометрических паспортов. Основным отличием электронных документов от существующих бумажных аналогов является специальный микрочип, на котором хранятся биометрические данные владельца паспорта. Используемая технология позволяет хранить на чипе до 19 биометрических характеристик человека. Заменить такой набор характеристик намного сложнее, чем напечатанные данные и соответственно намного сложнее выдавать себя за владельца паспорта. Вид казахстанского биометрического паспорта приведен на рис. 1.



Рис.1. Казахстанский биометрический паспорт

Главное преимущество электронного паспорта состоит в том, что на пунктах пограничного контроля некоторых стран установлено оборудование, считывающее данные с микрочипа. Такая процедура сокращает время ввода данных о лице, пересекающем границу, в пограничную систему. Благодаря хранению биометрических данных в паспорте, сравнение предъявителя паспорта и данных, хранящихся в паспорте (фотография лица, отпечатки пальцев и другие) выполняет автоматика. Такой подход снижает вероятность субъективной ошибки контролера, сокращает время идентификации и ускоряет процесс пограничного контроля.

Биометрические данные являются наиболее критичной информацией, доступ к которой долж-

ны получать исключительно те системы проверки, которые могут подтвердить свои полномочия на данные действия. Основными российскими нормативными документами по биометрической аутентификации являются ГОСТ Р ИСО/МЭК 19794-6 —2006 [1], ГОСТ Р ИСО/МЭК 19794-5 —2006[2], ГОСТ Р ИСО/МЭК 19794-2 —2005 [3], ГОСТ Р ИСО/МЭК 19794-4 —2006 [4], ГОСТ Р ИСО/МЭК 19785-1 —2008[5], ГОСТ Р ИСО/МЭК 19794-7 —2009 [6], ГОСТ Р ИСО/МЭК 19795-2 —2006 [7]. Стандарты устанавливают единицы измерения, состав и формат записи изображений, используемых для верификации и идентификации субъекта, условия получения изображений и др.

Основными источниками по вопросам биометрических паспортов являются публикации организации гражданской авиации ИКАО. Это, в первую очередь, Дос 9303 [8], который состоит из нескольких частей. Основной является часть 1 «Машиносчитываемые паспорта» том 2 «Спецификации на электронные паспорта со средствами биометрической идентификации».

Целью данной статьи является обоснование выбора и проведение сравнительного анализа основных методов биометрической идентификации, которые могут быть использованы в электронной паспортной системе и других машиносчитываемых документах.

1. ОСНОВЫ ПРИМЕНЕНИЯ БИОМЕТРИЧЕСКИХ ДАННЫХ

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

лицу. Идентификация на основе биометрических данных — это средство автоматического опознавания личности на базе уникальных физических или поведенческих параметров.

Считается, что эта методика вскоре станет главным конкурентом цифровым сертификатам и смарт-картам ввиду таких преимуществ:

1. Для биометрической идентификации достаточно физических параметров человека и не нужны никакие файлы (которые можно скопировать) или пароли (которые можно взломать). То есть идентификация происходит не по принципам «что-то знаю» (пароль) и «чем-то владею» (электронная карточка), а по принципу «что я есть» (физические параметры).

2. Уникальные человеческие признаки хороши тем, что их трудно подделать, трудно оставить фальшивый отпечаток пальца при помощи своего собственного или сделать радужную оболочку своего глаза похожей на чью-то другую.

3. В отличие от бумажных идентификаторов (паспорт, водительские права, удостоверение личности), от пароля или персонального идентификационного номера (ПИН), биометрические характеристики не могут быть забыты или потеряны, их всегда легко «предъявить».

Одним из главных показателей развития биометрии является стандартизация данной области [1-7, 9, 10]. Она идет по нескольким направлениям: как для отдельных областей, так и для всех способов биометрической идентификации в целом. Разработкой стандартов по биометрии занимаются государственные структуры, международные организации по стандартизации и независимые консорциумы, являющиеся объединением нескольких производителей.

В биометрических системах идентификационными являются индивидуальные особенности человека, которые в данном случае называются биометрическими признаками. Идентификация производится за счет сравнения полученных биометрических характеристик и хранящихся в базе шаблонов. В зависимости от характеристик, которые при этом используются, биометрические системы делятся на статические и динамические. Статическая биометрия основывается на данных (шаблонах), полученных путем измерения анатомических особенностей человека (отпечатки пальцев, узор радужки глаза и т.д.), а динамическая — на анализе действий человека (голос, параметры подписи, ее динамика).

В настоящее время активно используются следующие биометрические признаки [11]:

- отпечатки пальцев;
- геометрическая форма кисти руки;
- форма и размеры лица;
- особенности голоса;
- узор радужной оболочки и сетчатки глаз.

На рис. 2 приведены примеры таких биометрических данных: (а) — отпечаток пальца, (b) — лицо, (c) — радужная оболочка глаза, (d) —

расположение вен на лицевой стороне ладони, (e) — спектрограмма голоса, (f) — термограмма лица, (g) — 3-х мерное изображение лица, (h) — динамика набора на клавиатуре, (i) — ДНК.

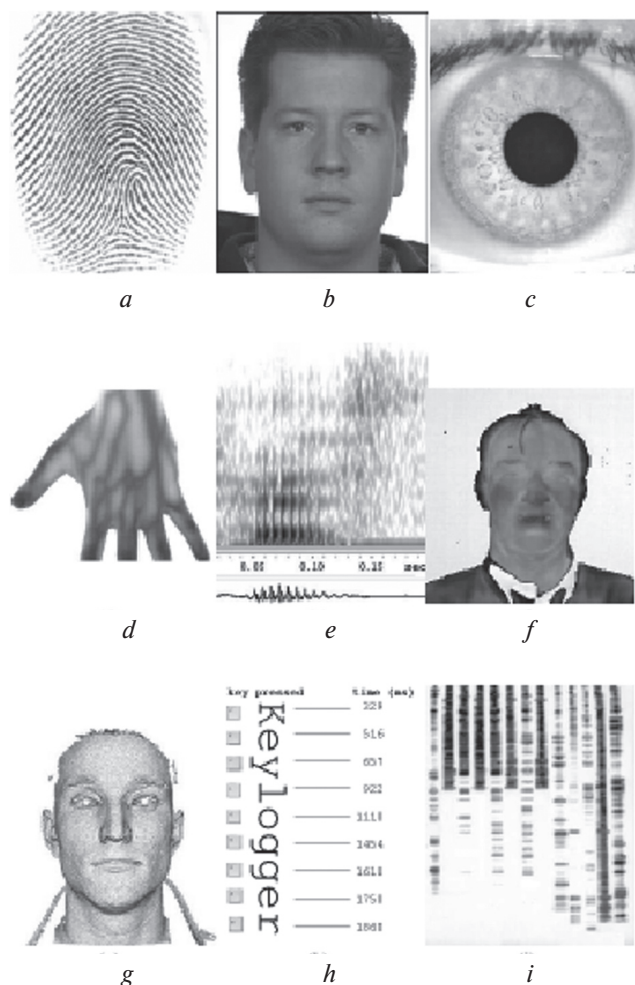


Рис. 2. Примеры разнообразных биометрических данных

2. СТАТИЧЕСКИЕ МЕТОДЫ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ

Уникальные физиологические, или по-другому статические характеристики каждого человеческого организма, которые он получает от Бога и природы, составляют основу статических методов биометрической аутентификации. Статические характеристики человека не меняются на протяжении всей его жизни и являются неотъемлемыми от него.

К методам этой группы относятся такие виды аутентификаций:

- 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 методы

Рассмотрим каждый из них подробнее.

По отпечатку пальца. Капиллярные узоры на пальцах человека уникальны. В этом и есть основа данного метода. Отпечаток, полученный с помощью специального сканера, преобразуется в цифровой код (свертку), и сравнивается с ранее введенным эталоном. Данная технология является самой распространенной по сравнению с другими методами биометрической аутентификации. Несмотря на то, что технология сканирования отпечатков пальцев является дешевой и достаточно точной, она не настолько однозначна как некоторые другие биометрические технологии. Считыватель отпечатков можно ввести в заблуждение, используя, например, латексные протезы пальцев, которые воспроизводят бы подлинный отпечаток. Некоторые считыватели также можно обмануть, сняв отпечатки пальцев с любой поверхности с помощью тонера к лазерным принтерам, а затем воспроизведя это изображение на фотобумаге. Другим недостатком метода является то, что некоторые инвалиды по понятным причинам не могут пользоваться такой технологией. Преимущества и недостатки данного метода приведены в табл. 1.

Таблица 1

Преимущества и недостатки метода идентификации по отпечатку пальца

Особенности	
Положительные	Отрицательные
Компактный считыватель. Низкая стоимость устройства. Небольшой процент ошибок. Простая процедура сканирования отпечатка.	Недостаточная защита от подделки отпечатка пальца. Узор отпечатка пальца легко изменяется царапинами

По форме ладони. Данный метод, построен на геометрии кисти руки. С помощью специального устройства, состоящего из камеры и нескольких подсвечивающих диодов (включаясь по очереди, они дают разные проекции ладони), строится трехмерный образ кисти руки, по которому формируется свертка и распознается человек. Преимущества и недостатки данного метода приведены в табл. 2.

Таблица 2

Преимущества и недостатки метода идентификации по геометрии кисти руки

Особенности	
Положительные	Отрицательные
Стойкий параметр. Простота алгоритма идентификации. Небольшой идентификационный код.	Громоздкий считыватель. Рассчитан на правую руку. Используется только с PIN-кодом. Непосредственный контакт с оборудованием

По расположению вен на лицевой стороне ладони. С помощью инфракрасной камеры считывается

рисунок вен на лицевой стороне ладони или кисти руки, полученная картинка обрабатывается и по схеме расположения вен формируется цифровая свертка.

По сетчатке глаза. Вернее этот способ идентификации по рисунку кровеносных сосудов глазного дна. Для того, чтобы этот рисунок стал виден человеку, нужно посмотреть на удаленную световую точку, и таким образом подсвеченное глазное дно сканируется специальной камерой.

По радужной оболочке глаза. Рисунок радужной оболочки глаза также является уникальной характеристикой человека. При этом для ее сканирования достаточно портативной камеры со специализированным программным обеспечением, позволяющим захватывать изображение части лица, из которого выделяется изображение глаза. Из изображения глаза выделяется рисунок радужной оболочки, по которому строится цифровой код для идентификации человека. Технология даже превосходит точность анализа ДНК, который дорого и неудобно использовать для аутентификации. Во время сканирования радужки служит своего рода «штрих-кодом человека», поскольку обладает уникальным рисунком – запутанной сеткой соединительной ткани и других видимых особенностей.

Считается, что у разных людей не может быть двух похожих радужек, даже у однояйцовых близнецов. Крупнейшим недостатком идентификации по радужке является высокая цена устройств. Так же, как и в случае со считывателями отпечатков пальцев, необходимо предусмотреть способ аутентификации для инвалидов – людей, чьи радужки невозможно сканировать. Преимущества и недостатки данного метода приведены в табл. 3.

Таблица 3

Преимущества и недостатки метода идентификации по радужной оболочке глаза

Особенности	
Положительные	Отрицательные
Очень сложно подделать. Отсутствие непосредственного контакта с оборудованием. Защита от повреждений роговицей.	Сравнительно большая стоимость устройства

По форме лица. В данном методе идентификации строится трехмерный образ лица человека. На лице выделяются контуры бровей, глаз, носа, губ и т.д., вычисляется расстояние между ними и строится не просто образ, а еще множество его вариантов на случаи поворота лица, наклона, изменения выражения. Количество образов варьирует в зависимости от целей использования данного способа (для аутентификации, верификации, удаленного поиска на больших территориях и т.д.). Это популярная биометрическая технология. Она пассивна, люди могут быть отсканированы без их ведома. Многие казино и различные спецслужбы используют камеры безопасности для распозна-

вания лиц и выявления нежелательных персон или правонарушителей. Преимущества и недостатки данного метода приведены в табл. 4.

Таблица 4

Преимущества и недостатки метода идентификации по 3-х мерному изображению лица

Особенности	
Положительные	Отрицательные
Отсутствие непосредственного контакта с оборудованием. Независимость от освещения, положения головы, наличия очков и др. Достаточно высокий уровень надежности	Высокая стоимость устройства. Много алгоритмов не учитывают мимику.

По термограмме лица. В основе данного способа аутентификации лежит уникальность распределения на лице артерий, которые выделяют тепло. Для получения термограммы, используются специальные камеры инфракрасного диапазона. В отличие от предыдущего, этот метод позволяет различать близнецов.

По ДНК. Преимущества данного способа очевидны, однако используемые в настоящее время методы получения и обработки ДНК работают долго и требуют больших денежных затрат. Так что такие системы используются только для специализированных экспертиз.

Другие методы. На самом деле здесь описаны только самые распространенные методы, существуют еще такие уникальные способы — как идентификация по подногтевому слою кожи, по объему указанных для сканирования пальцев, форме уха, запаху тела и т.д.

3. ДИНАМИЧЕСКИЕ МЕТОДЫ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ

Динамические методы биометрической аутентификации основываются на поведенческой (динамической) характеристике человека, т.е. построены на особенностях, характерных для подсознательных движений в процессе воспроизведения какого-либо действия.

К методам этой группы относятся такие виды аутентификаций:

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

Рассмотрим подробнее каждый из них.

По рукописному почерку. Как правило, для этого вида идентификации человека используется его роспись (иногда написание кодового слова). Существует два вида цифрового кода идентификации, в зависимости от необходимой степени защиты и наличия оборудования (графический планшет, экран карманного компьютера Palm и т.д.):

1. По самой росписи, то есть для идентификации используется просто степень совпадения двух картинок.

2. По росписи и динамическим характеристикам написания, то есть для идентификации строится свертка, в которую входит информация по непосредственно подписи, временным характеристикам нанесения росписи и статистическим характеристикам динамики нажима на поверхность.

Преимущества и недостатки данного метода приведены в табл. 5.

Таблица 5

Преимущества и недостатки метода идентификации по рукописному почерку

Особенности	
Положительные	Отрицательные
Небольшая стоимость устройства. Используется во всех сферах жизнедеятельности.	Возможна подделка. Проблема выбора разметки подписи. Зависит от психологического состояния человека и стабильности почерка.

По клавиатурному почерку. Метод в целом аналогичен выше описанному, но вместо росписи используется некое кодовое слово (когда для этого используется личный пароль пользователя, такую аутентификацию называют двухфакторной) и не нужно никакого специального оборудования, кроме стандартной клавиатуры. Основная характеристика, по которой строится свертка для идентификации — динамика набора кодового слова.

По голосу. Одна из старейших технологий, в настоящее время ее развитие ускорилося — так как предполагается ее широкое использование в построении «интеллектуальных зданий». Существует достаточно много способов построения кода идентификации по голосу, как правило, это различные сочетания частотных и статистических характеристик голоса. Преимущества и недостатки данного метода приведены в табл. 6.

Таблица 6

Преимущества и недостатки метода идентификации по голосу

Особенности	
Положительные	Отрицательные
Относительно небольшая стоимость устройства. Распространенный метод.	Небольшая гибкость метода: даже небольшой ларингит или кашель меняют голос. Голос может записать, а потом воспроизвести 3-я сторона.

Другие методы. Для данной группы методов также описаны только самые распространенные методы, существуют еще такие уникальные способы как идентификация по движению губ при воспроизведении кодового слова, по динамике поворота ключа в дверном замке и т.д.

4. БИОМЕТРИЧЕСКИЕ СИСТЕМЫ АУТЕНТИФИКАЦИИ

В общем случае биометрические системы аутентификации работают в двух режимах:

1. *Режим регистрации.* В этом режиме происходит получение пользовательских данных. Это делается с помощью некоторых типов биометрических считывающих устройств. После этого собранная информация сохраняется в базе данных вместе с личными данными пользователя (имя, идентификационный номер и т.п.) для облегчения процесса аутентификации [12].

2. *Режим аутентификации.* Полученные биометрические данные используются системой для проверки того, тем ли является пользователь, за кого он себя выдает. Это происходит при помощи сравнения биометрических данных пользователя с базой данных. Если заявленные данные присутствуют в базе данных, то такой пользователь принимается за истинного и наоборот.

В общем случае любая биометрическая система состоит из таких компонент:

- *Сенсорный модуль.* Этот модуль получает биометрические данные пользователя. Примером такого модуля могут служить сканеры отпечатков пальцев.

- *Модуль извлечения биометрических характеристик.* Этот модуль предназначен для извлечения основных значений биометрических характеристик. Так, к примеру, если в качестве биометрического признака будет геометрия руки, то на данном этапе будут вычисляться значения ширины и длины пальцев, толщины ладони и др.

- *Модуль сравнения.* Данный модуль сравнивает полученные биометрические характеристики с теми, которые хранятся в базе данных.

- *Модуль принятия решений.* Пользовательская идентичность подтверждается или опровергается. Это происходит на основании результатов модуля сравнений.

Схема работы данных модулей приведена на рис. 3.

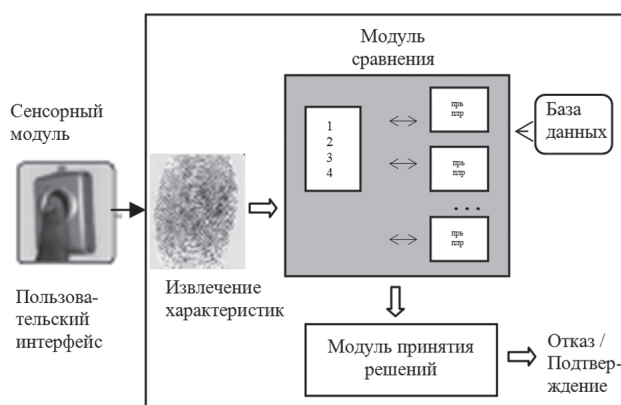


Рис. 3. Схема работы биометрической системы аутентификации

Модуль принятия решений может совершать два вида ошибок. Ошибки, которые могут быть сделаны в процессе верификации называются:

- False Rejection (FR) – это отказ в доступе клиенту, имеющему право доступа.
- False Acceptance (FA) – это когда система ошибочно опознает чужого как своего.

5. ОЦЕНКА ПРОИЗВОДИТЕЛЬНОСТИ

Оценка систем биометрической аутентификации производится на основании ошибок первого (FRR) и второго (FAR) рода. 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. Вычисление их производится по формулам:

$$FRR = \frac{\text{общее число ложных отказов в доступе}}{\text{общее число тестируемых объектов}} \quad (1)$$

$$FAR = \frac{\text{общее число ложных доступов}}{\text{общее число тестируемых объектов}} \quad (2)$$

Показатель истинного принятия (Genuine Accept Rate – GAR) – это вероятность истинного принятия пользователя, имеющего право доступа:

$$GAR = 1 - FRR. \quad (3)$$

В идеальном варианте система биометрической аутентификации имела бы FAR=0 и FRR=0. Однако, такие значения в реальности не достижимы. Значение любой из двух ошибок возможно уменьшить. Недостаток этого в том, что второе значение возрастет. Обычно системные параметры настраивают так, чтобы добиться требуемого коэффициента ошибочных подтверждений, что определяет соответствующий коэффициент ошибочных отказов.

Если систему необходимо охарактеризовать одним критерием, то используется коэффициент равной вероятности ошибок 1-го и 2-го (EER – Equal Error Rates), который является точкой совпадения вероятностей FRR и FAR. Качественная и надежная система должна иметь низкий уровень EER.

На рис. 4 показаны графики ошибок первого и второго рода, а также коэффициент равной вероятности ошибок EER для метода идентификации по рукописной подписи [13].

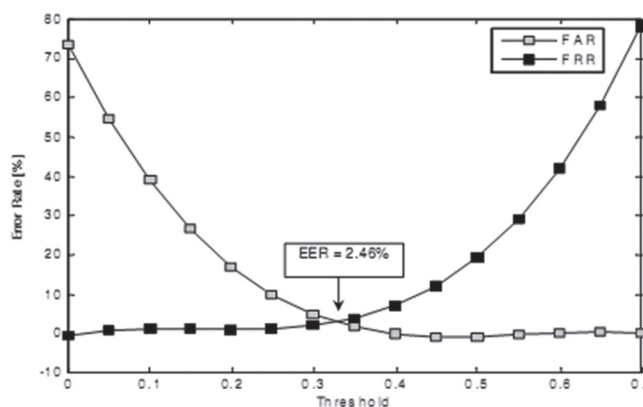


Рис. 4. Графики FAR и FRR для метода биометрической идентификации по рукописной подписи

6. ОСНОВНЫЕ ПРОБЛЕМЫ И ЗАДАЧИ В ОБЛАСТИ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ

Из недостатков биометрической аутентификации можно отметить следующие [14]:

- отсутствие хорошо подготовленного профессионального персонала;
- высокая стоимость некоторых устройств биометрической аутентификации;
- сложность настройки таких систем;
- противодействие со стороны сотрудников, так как руководство получает возможность контролировать все их перемещения и фактически производить контроль рабочего времени;
- невозможно применять для идентификации людей с некоторыми физическими недостатками;
- возможность воспользоваться муляжом (к примеру, отпечатка пальца);
- нестандартный рост (менее 1,55 м или более 2,1 м). Сканирование лица может стать затруднительным.

Исходя из анализа недостатков биометрической аутентификации, сформулируем основные проблемные задачи, которые необходимо разрешить:

- подготовка высококвалифицированного персонала;
- минимизирование стоимости биометрических устройств, создание бюджетной линейки товаров;

- упрощение настройки биометрических систем;
- работа с персоналом по популяризации данного направления;
- адаптация биометрических систем для идентификации людей с некоторыми физическими недостатками;
- усовершенствование систем биометрической идентификации для исключения возможности воспользоваться муляжом.

7. СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ

Сравнительный анализ методов биометрической аутентификации производился на основании ошибок первого и второго рода, а также коэффициента равной вероятности ошибок (EER). Также учитывались преимущества и недостатки рассматриваемых методов. Сравнение производилось по следующим биометрическим параметрам: отпечаток пальца, геометрическая форма кисти руки, радужная оболочка глаза, 3-х мерное изображение лица, рукописная подпись, голос.

Результаты сравнений приведены в табл. 7.

ВЫВОДЫ

Биометрические технологии аутентификации имеют большие перспективы развития. При использовании систем на основании биометрических методов процедуры доступа становятся

Таблица 7

Сравнительный анализ биометрических методов аутентификации

Биометрический параметр	Цена устройства в \$	Ошибки I, II рода и значение EER в %	Особенности	
			Положительные	Отрицательные
Отпечаток пальца	Около 100\$	FRR = 0,01 - 0,0001 FAR = 0,002 - 0,0001. EER = 0,01	Компактный считыватель. Низкая стоимость устройства. Небольшой процент ошибок. Простая процедура сканирования отпечатка.	Недостаточная защита от подделки отпечатка пальца. Узор отпечатка пальца легко изменяется царапинами
Геометрическая форма кисти руки	От 600\$	FRR = 0,001 FAR = 0,000001 EER = 0,1-0,5	Стойкий параметр. Простота алгоритма идентификации. Небольшой идентификационный код.	Громоздкий считыватель. Рассчитан на правую руку. Используется только с PIN- кодом. Непосредственный контакт с оборудованием.
Радужная оболочка глаза	От 500\$	FRR = 0,009 FAR = $1 \cdot 10^{-6}$ EER = 0,0021	Очень сложно подделать. Отсутствие непосредственного контакта с оборудованием. Защищена от повреждений роговицей.	Сравнительно большая стоимость устройства.
3-х мерное изображение лица	Около 4000\$	FRR = 0,103. FAR = 0,0047 EER = 0,75	Отсутствие непосредственного контакта с оборудованием. Независимость от освещения, положения головы, наличия очков и др. Достаточно высокий уровень надежности.	Высокая стоимость устройства. Много алгоритмов не учитывают мимику.
Рукописная подпись	От 200\$	EER = 2,46	Небольшая стоимость устройства. Используется во всех сферах жизнедеятельности.	Возможна подделка. Проблема выбора разметки подписи. Зависит от психологического состояния человека и стабильности почерка.
Голос	Около 400\$	EER ~ 2 - 5	Относительно небольшая стоимость устройства. Распространенный метод.	Небольшая гибкость метода: даже небольшой ларингит или кашель меняют голос. Голос может записать, а потом воспроизвести 3-я сторона.

быстрее, безопаснее и проще. Но, несмотря на огромное количество преимуществ, биометрические технологии имеют ряд сложностей и проблем. Так, необходимо решать вопросы по использованию устройств биометрической идентификации людьми с некоторыми физическими недостатками, по подготовке профессиональных кадров, уменьшению стоимости устройств и др.

Внедрение биометрических паспортов является приоритетным направлением в развитии международных отношений. Использование биометрических технологий в паспортной системе позволяет намного упростить процедуру идентификации, снизить вероятность субъективной ошибки контролера, ускорить процесс пограничного контроля. В электронный паспорт может быть записано до 19 биометрических характеристик человека.

На основании проведенного анализа, можно сделать вывод о том, что самым точным и наилучшим методом биометрической аутентификации для использования в электронной паспортной системе является аутентификация по радужной оболочке глаза. Как дополнительный параметр, возможно использовать отпечаток пальца или геометрическую форму кисти руки.

Литература

- [1] Стандарт ГОСТ Р ИСО/МЭК 19794-6-2006. Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки глаза.
- [2] Стандарт ГОСТ Р ИСО/МЭК 19794-5 — 2006. Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица.
- [3] Стандарт ГОСТ Р ИСО/МЭК 19794-2 — 2005. Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца — контрольные точки.
- [4] Стандарт ГОСТ Р ИСО/МЭК 19794-4 — 2006. Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальца.
- [5] Стандарт ГОСТ Р ИСО/МЭК 19785-1 — 2008. Автоматическая идентификация. Идентификация биометрическая. Единая структура форматов обмена биометрическими данными. Часть 4. Спецификация элементов данных.
- [6] Стандарт ГОСТ Р ИСО/МЭК 19794-7 — 2009. Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 7. Данные динамики подписи.
- [7] Стандарт ГОСТ Р ИСО/МЭК 19795-2 — 2006. Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 2. Методология проведения технологического и сценарного испытаний.
- [8] ICAO 9303- : 9303 part 1 volume 2, Sixth edition, 2006, Specifications for Electronically Enabled Passports with Biometric Identification Capability.
- [9] ISO/IEC 19794-5 Information technology — Biometric data interchange formats — Part 5: Face image data.
- [10] ISO/IEC 19794-6 Information technology — Biometric data interchange formats — Part 6: Iris image data.
- [11] Технологии аутентификации [Электронный ресурс]. — 2009. — Режим доступа: <http://ypn.ru/category/data-protection-technologies/authentication-technologies/>
- [12] Jain A. K., Ross A. Information fusion in biometrics. — Pattern Recognition Letters, Vol. 4, pp. 2115-2125, 2003.
- [13] Sayeed S., Kamel N. S., Besar R. A Sensor-Based Approach for Dynamic Signature Verification using Data Glove, 2009.
- [14] Безмальный В. Парольная защита: прошлое, настоящее, будущее / В. Безмальный // Компьютер Пресс 9. — Россия, 2008.

Поступила в редколлегию 24.05.2011



Горбенко Иван Дмитриевич, профессор, зав. кафедрой БИТ ХНУРЭ, главный конструктор ЗАО «ИИТ». Область научных интересов: проектирование и разработка средств КЗИ.



Олешко Инна Викторовна, аспирант каф. БИТ ХНУРЭ. Область научных интересов: электронная паспортная система, биометрическая аутентификация.

УДК 621.391:519.2:519.7

Методи біометричної автентифікації для використання в паспортній системі / І.Д. Горбенко, І.В. Олешко // Прикладна радіоелектроніка: наук.-техн. журнал. — 2011. Том 10. № 2. — С. 233—239.

У роботі розглядаються методи біометричної автентифікації. Наводяться критерії оцінки біометричних систем. Даються рекомендації по використанню біометричних методів в паспортній системі.

Ключові слова: біометричний паспорт, біометрична ідентифікація, статична біометрія, динамічна біометрія, коефіцієнт рівної імовірності помилок, біометрична система автентифікації.

Табл. 7. Іл. ..4. Бібліогр.: 14 найм.

UDC 621.391:519.2:519.7

Methods of biometric authentication for the use in the passport system / I.D. Gorbenko, I.V. Oleshko // Applied Radio Electronics: Sci. Journ. — 2011. Vol. 10. № 2. — P. 233—239.

The paper examines the methods of biometric authentication. Criteria of estimating biometric systems are given. Recommendations on the use of biometric methods in the passport system are provided.

Keywords: biometrical passport, biometrical authentication, static biometrics, dynamic biometrics, coefficient of equal probability of errors, biometrical authentication system.

Tab. 7. Fig. 4. Ref.: 14 items.