

СОВРЕМЕННЫЕ БИОМЕТРИЧЕСКИЕ МЕТОДЫ ИДЕНТИФИКАЦИИ

Василий МОРЖАКОВ,

ген. директор ООО «Динамика»,

Антон МАЛЬЦЕВ,

инженер ООО «Динамика»

Технология биометрической идентификации уже заняла прочные позиции на рынке систем безопасности благодаря ее основному достоинству — производится идентификация физиологических особенностей человека, а не ключа или карточки. В статье будут рассмотрены характеристики и ограничения различных биометрических методов, а также уровень их развития сегодня.

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 видекамера, на него можно установить систему распознавания человека по лицу.

Обилие биометрических методов поражает. Основными методами, использующими статистические биометрические характеристики человека, являются идентификация по папиллярному рисунку на пальцах, радужной оболочке, геометрии лица, сетчатке глаза человека, рисунку вен руки. Также существует ряд методов, использующих динамические характеристики человека: идентификация по голосу, динамике рукописного подчерка, сердечному ритму, походке.

В данной статье будут рассмотрены сравнительные характеристики статических биометрических методов в связи с их большей статистической надежностью и более высоким уровнем развития по сравнению с динамическими методами. В качестве сравнительных характеристик использованы следующие показатели: FRR при фиксированном значении FAR, устойчивость к подделке, устойчивость к окружающей среде, простота использования, стоимость, скорость, изменчивость характеристики во времени.

Основными характеристиками любой биометрической охранной системы являются два числа — FAR (False Acceptance Rate) и FRR (False Rejection Rate). Первое число характеризует вероятность ложного совпадения биометрических характеристик двух людей. Второе — вероятность отказа доступа человеку, имеющего допуск. Система тем лучше, чем меньше значение FRR при одинаковых значениях FAR. Устойчивость к подделке — это эмпирическая характеристика, обобщающая то, насколько легко обмануть биометрический идентификатор. Устойчивость к окружающей среде — характеристика, эмпирически оценивающая устойчивость работы системы при различных внешних условиях. Простота использования показывает, насколько сложно воспользоваться биометрическим сканером, возможна ли идентификация «на ходу». Важными характеристиками являются и скорость работы, и стоимость системы. Несомненно, существенным является и то, как в течение времени себя ведет биометрическая характеристика. Если она неустойчива и может измениться — это значительный минус.

В статье будут описаны уровни развития каждой из технологий и сложности, с которыми сталкиваются при создании различных систем.

Отпечатки пальцев

Дактилоскопия (распознавание отпечатков пальцев) — наиболее разработанный на сегодняшний день биометрический метод идентификации личности. Катализатором развития метода послужило его широкое использование в криминалистике XX века.

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

Статистические характеристики метода

В качестве источника данных по FAR и FRR использовались статистические данные VeriFinger SDK, полученные при помощи сканера отпечатков пальцев DP U.are.U.

Характерное значение FAR для метода распознавания отпечатков пальцев — 0,001%.

FAR	FRR
0,1%	0,3%
0,01%	0,4%
0,001%	0,6%
0,0001%	0,9%

Таб. 1.

Чтобы ощутить эту вероятность, можно оценить, как часто будет возникать ложные совпадения, если установить систему идентификации на проходной организации с численностью персонала N человек. Вероятность ложного совпадения, полученного сканером отпечатка пальца для базы данных из N отпечатков, равна $FAR \times N$. И каждый день через пункт контроля доступа проходит тоже порядка N человек. Тогда вероятность ошибки за рабочий день $FAR \times N^2$. Конечно, в зависимости от целей системы идентификации вероятность ошибки за единицу времени может сильно варьироваться, но если принять допустимым одну ошибку в течение рабочего дня, то:

$$FAR \times N^2 \approx 1 \Rightarrow N \approx \sqrt{\frac{1}{FAR}} \quad (1)$$

Тогда получим, что стабильная работа системы идентификации при FAR = 0,001% возможна при численности персонала $N \approx 300$.

Преимущества и недостатки метода

Преимущества метода	Недостатки метода
<ul style="list-style-type: none"> • высокая достоверность — статистические показатели метода выше показателей способов идентификации по лицу, голосу, росписи; • низкая стоимость устройств, сканирующих изображение отпечатка пальца; • достаточно простая процедура сканирования отпечатка. 	<ul style="list-style-type: none"> • папиллярный узор отпечатка пальца очень легко повреждается мелкими царапинами, порезами; • недостаточная защищенность от подделки изображения отпечатка, отчасти вызванная широким распространением метода.

Таб. 2.

Радужная оболочка

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

Система идентификации личности по радужной оболочке логически делится на две части: устройство захвата изображения, его первичной обработки и передачи вычислителю; вычислитель, производящий сравнение изображения с изображениями в базе данных, передающий команду о допуске исполнителю устройству.

Время первичной обработки изображения в современных системах примерно 300–500 мс, скорость сравнения полученного изображения с базой имеет уровень 50000–150000 сравнений в секунду даже на обычном персональном компьютере. Такая скорость сравнения не накладывает ограничений на применение метода в больших организациях при использовании в системах доступа. При использовании же специализированных вычислителей и алгоритмов оптимизации поиска становится даже возможным идентифицировать человека среди жителей целой страны.

Статистические характеристики метода

Характеристики FAR и FRR для радужной оболочки глаза наилучшие в классе современных биометрических систем (за исключением, возможно, метода распознавания по сетчатке глаза). В статье приведены характеристики библиотеки распознавания радужной оболочки глаза российской разработки — EyeR SDK, — полученные на открытых базах глаз фирмы CASIA.

FAR	FRR (Casia 1)	FRR (Casia 3)
0,1%	0,05%	0,08%
0,01%	0,05%	0,09%
0,001%	0,13%	0,10%
0,0001%	0,13%	0,17%
0,00001%	0,13%	0,19%

Таб. 3.

Характерное значение FAR — 0,00001%.

$$N \approx \sqrt{\frac{1}{FAR}} \approx 3000$$

численность персонала организации, при которой идентификация сотрудника происходит достаточно стабильно.

Здесь стоит отметить немаловажную особенность, отличающую систему распознавания по радужной оболочке от других

систем. В случае использования камеры разрешения от 1.3 мегапикс. можно захватывать два глаза на одном кадре. Так как вероятности FAR и FRR являются статистически независимыми вероятностями, то при распознавании по двум глазам значение FAR будет приблизительно равняться квадрату значения FAR для одного глаза. Например, для FAR 0,001% при использовании двух глаз вероятность ложного допуска будет равна 10–8 %, при FRR — всего в 2 раза выше, чем соответствующее значение FRR для одного глаза при FAR = 0,001%.

Преимущества и недостатки метода:

Преимущества метода	Недостатки метода
<ul style="list-style-type: none"> • статистическая надежность метода; • захват изображения радужной оболочки можно производить на расстоянии от нескольких сантиметров до нескольких метров, при этом физический контакт человека с устройством не происходит; • радужная оболочка защищена от повреждений роговицей (например, отпечатки пальцев легко портятся царапинами или пачкаются); • большое количество методов противодействия подделкам. 	<ul style="list-style-type: none"> • цена системы для захвата радужной оболочки выше стоимости сканера отпечатка пальца и камеры для захвата 2D изображения лица.

Таб. 4.

Геометрия лица

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

2D-распознавание лица

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

Статистические характеристики метода

Для FAR и FRR использованы данные для алгоритмов VeriLook.

FAR	FRR
0,1%	2,5%
0,01%	5%
0,001%	6%
0,0001%	9%

Таб. 5.

Характерное значение FAR — 0,1%.

Из формулы (1) получаем $N \approx 30$ — численность персонала организации, при которой идентификация сотрудника происходит достаточно стабильно.

Как видно, статистические показатели метода достаточно скромные, и это нивелирует то преимущество метода, что можно проводить скрытую съемку лиц в людных местах. И безуспеш-

ные попытки применять этот метод для обнаружения преступников в местах скопления людей по изображениям, полученным с видеокамер, в немалой степени дискредитировали этот метод на раннем этапе его развития.

Преимущества и недостатки метода

Преимущества метода	Недостатки метода
<ul style="list-style-type: none"> • при 2D-распознавании, в отличие от большинства биометрических методов, не требуется дорогостоящее оборудование; • возможность распознавания на значительных расстояниях от камеры. 	<ul style="list-style-type: none"> • низкая статистическая достоверность; • предъявляются требования к освещению (например, не удастся регистрировать лица входящих с улицы людей в солнечный день); • для многих алгоритмов неприемлемость каких-либо внешних помех, как, например, очки, борода, некоторые элементы прически; • обязательно фронтальное изображение лица, с весьма небольшими отклонениями; • многие алгоритмы не учитывают возможные изменения мимики лица, т. е. выражение должно быть нейтральным.

Таб. 6.

3D-распознавание лица

Реализация данного метода представляет собой довольно сложную задачу. Несмотря на это, в настоящее время существует множество методов по 3D-распознаванию лица. Ниже рассматривается один из самых распространенных.

Метод проецирования шаблона состоит в том, что на объект (лицо) проецируется сетка. Далее камера делает снимки со скоростью десятки кадров в секунду, и полученные изображения обрабатываются специальной программой. Луч, падающий на искривленную поверхность, изгибается — чем больше кривизна поверхности, тем сильнее изгиб луча. Изначально при этом применялся источник видимого света, подаваемого через «жалюзи». Затем видимый свет был заменен инфракрасным, который обладает рядом преимуществ. Обычно на первом этапе обработки отбрасываются изображения, на которых лица не видно вообще или присутствуют посторонние предметы, мешающие идентификации. По полученным снимкам восстанавливается 3D-модель лица, на которой выделяются и удаляются ненужные помехи (прическа, борода, усы и очки). Затем производится анализ модели — выделяются антропометрические особенности, которые в итоге и записываются в уникальный код, заносимый в базу данных. Время захвата и обработки изображения составляет 1–2 с для лучших моделей.

Статистические показатели метода

Полные данные о FRR и FAR для алгоритмов этого класса на сайтах производителей открыто не приведены. Но для лучших моделей фирмы Bioscript (3D EnrolCam, 3D FastPass) при FAR=0,0047% FRR составляет 0,103%.

Считается, что статистическая надежность метода сравнима с надежностью метода идентификации по отпечаткам пальцев.

Преимущества и недостатки метода

Преимущества метода	Недостатки метода
<ul style="list-style-type: none"> • отсутствие необходимости контактировать со сканирующим устройством; • низкая чувствительность к внешним факторам, как на самом человеке (появление очков, бороды, изменение прически), так и в его окружении (освещение, поворот головы); • высокий уровень надежности, сравнимый с методом идентификации по отпечаткам пальцев. 	<ul style="list-style-type: none"> • дороговизна оборудования; • изменения мимики лица и помехи на лице ухудшают статистическую надежность метода; • метод еще недостаточно хорошо разработан, особенно в сравнении с давно применяющейся дактилоскопией, что затрудняет его широкое применение.

Таб. 7.

Венозный рисунок руки

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

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

Значение FRR и FAR приведено для сканера Palm Vein. Согласно данным разработчика, при FAR 0,0008% FRR составляет 0,01%.

Преимущества и недостатки метода

Преимущества метода	Недостатки метода
<ul style="list-style-type: none"> • отсутствие необходимости контактировать со сканирующим устройством; • высокая достоверность — статистические показатели метода сравнимы с показателями радужной оболочки. 	<ul style="list-style-type: none"> • недопустима засветка сканера солнечными лучами и лучами галогеновых ламп; • некоторые возрастные заболевания, например артрит, сильно ухудшают FAR и FRR; • метод менее изучен в сравнении с другими статическими методами биометрии.

Таб. 8.

Сетчатка глаза

До последнего времени считалось, что самый надежный метод биометрической идентификации личности — это метод, основанный на сканировании сетчатки глаза. Он содержит в себе лучшие черты идентификации по радужной оболочке и по венам руки. Сканер считывает рисунок капилляров на поверхности сетчатки глаза. Сетчатка имеет неподвижную структуру, неизменную во времени, кроме как в результате глазной болезни, например, катаракты.

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 системах контроля доступа на особо секретные объекты, так как у них один из самых низких процентов отказа в доступе зарегистрированных пользователей и практически не бывает ошибочного разрешения доступа.

К сожалению, целый ряд трудностей возникает при использовании этого метода биометрии. Сканером тут является весьма сложная оптическая система, а человек должен значительное время не двигаться, пока система наводится, что вызывает неприятные ощущения.

По данным компании EyeDentify, для сканера ICAM2001 при FAR=0,001% значение FRR составляет 0,4%.

Преимущества и недостатки метода:

Преимущества метода	Недостатки метода
<ul style="list-style-type: none"> • высокий уровень статистической надежности; • из-за низкой распространенности систем мала вероятность разработки способа их «обмана»; • бесконтактный метод снятия данных. 	<ul style="list-style-type: none"> • сложная при использовании система с долгим временем обработки; • высокая стоимость системы; • отсутствие широкого рынка предложения и, как следствие, недостаточная интенсивность развития метода.

Таб. 9.

Ситуация на рынке биометрических технологий

С конца 90-х годов XX века мировой рынок биометрии достаточно активно развивается. Необходимость новых решений в области безопасности несомненна. Различные предприятия, учреждения, банки нуждаются в системах контроля управления доступом. И именно биометрические решения вызывают сейчас наибольший интерес в этой сфере.

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

На российском рынке, по прогнозам экспертов, доля биометрических систем в ближайшие годы будет составлять значительную часть от общего рынка систем безопасности. Здесь также первое место будет занимать распознавание по отпечаткам пальцев. Идентификация по геометрии лица тоже имеет место на российском рынке, однако предпочтение отдается все-таки дактилоскопическому методу как наиболее изученному. А вот остальные методы биометрии в России производителями пока что практически не представлены.

Отпечатки пальцев

Как мы уже сказали, на данный момент системы распознавания по отпечаткам пальцев занимают более половины биометрического рынка. Множество российских и зарубежных компаний занимаются производством систем управления доступом, основанных на методе дактилоскопической идентификации. По причине того, что это направление является одним из самых давних, оно получило наибольшее распространение и является на сегодняшний день самым разработанным. Сканеры отпечатков пальцев прошли действительно длинный путь к улучшению. Современные системы оснащены различными датчиками (температуры, силы нажатия и т.п.), которые повышают степень защиты от подделок. С каждым днем системы становятся все более удобными и компактными. По сути, разработчики достигли уже некоего предела в данной области, и развивать метод дальше некуда. Кроме того, большинство компаний производят готовые системы, которые оснащены всем необходимым, включая программное обеспечение. Интеграторам в этой области просто нет необходимости собирать систему самостоятельно, так как это невыгодно и займет больше времени и сил, чем купить готовую и уже недорогую при этом систему, тем более выбор будет действительно широк.

Среди зарубежных компаний, занимающихся системами распознавания по отпечаткам пальцев, можно отметить SecuGen (USB-сканеры для PC, сканеры, которые можно устанавливать на предприятия или встраивать в замки, SDK и ПО для связи системы с компьютером); Bayometric Inc. (fingerprint scanners, TAA/Access control systems, fingerprint SDKs, embedded fingerprint modules); DigitalPersona, Inc. (USB-scanners, SDK). В России в данной области работают компании BioLink (дактилоскопические сканеры, биометрические устройства управления доступом, ПО); «Сонда» (дактилоскопические сканеры, биометрические устройства управления доступом, SDK); «СмартЛок» (дактилоскопические сканеры и модули) и др.

Геометрия лица

Распознавание по геометрии лица причисляют к «трем большим биометрикам» вместе с распознаванием по отпечат-

кам пальцев и радужной оболочке. Надо сказать, что данный метод довольно распространен, и ему отдают пока предпочтение перед распознаванием по радужке глаза. Удельный вес технологий распознавания по геометрии лица в общем объеме мирового биометрического рынка можно оценивать в пределах 13–18%. В России к данной технологии также проявляется большой интерес, чем, например, к идентификации по радужной оболочке. Как уже упоминалось ранее, существует множество алгоритмов 3D-распознавания. В большинстве своем компании предпочитают развивать готовые системы, включающие сканеры, сервера и ПО. Однако есть и те, кто предлагает потребителю только SDK. На сегодняшний день можно отметить следующие компании, занимающиеся развитием данной технологии: Geometrix, Inc. (3D-сканеры лица, ПО), Genex Technologies (3D-сканеры лица, ПО) в США, Cognitec Systems GmbH (SDK, специальные вычислители, 2D-камеры) в Германии, Bioscrypt (3D-сканеры лица, ПО) — дочернее предприятие американской компании L-1 Identity Solutions.

В России в данном направлении работает компания Artes Group (3D-сканеры лица и ПО) — компания, головной офис которой находится в Калифорнии, а разработки и производство ведутся в Москве. Также несколько российских компаний владеют технологией 2D-распознавания лица — Vocord, ITV и др.

В области распознавания 2D-лица основным предметом разработки является программное обеспечение, так как обычные камеры отлично справляются с захватом изображения лица. Решение задачи распознавания по изображению лица в какой-то степени зашло в тупик — уже на протяжении нескольких лет практически не происходит улучшения статистических показателей алгоритмов. В этой области происходит планомерная «работа над ошибками».

3D-распознавание лица сейчас является куда более привлекательной областью для разработчиков. Хотя этот метод и остается достаточно закрытым, но технические сложности на пути создания 3D-сканера вполне решаемы. Скорее всего, тормозящие факторы развития этой технологии в России — это отсутствие на рынке самостоятельного программного обеспечения распознавания и сложностей, которые могут возникнуть при продвижении продукта на рынок.

Радужная оболочка глаза

На данный момент удельный вес технологий идентификации по радужной оболочке глаза на мировом биометрическом рынке составляет по разным подсчетам от 6 до 9% (в то время как технологии распознавания по отпечаткам пальцев занимают свыше половины рынка). Следует отметить, что с самого начала развития данного метода его укрепление на рынке замедляла высокая стоимость оборудования и компонентов, необходимых, чтобы собрать систему идентификации. Однако по мере развития цифровых технологий себестоимость отдельной системы стала снижаться.

Лидером по разработке ПО в данной области является компания Iridian Technologies.

Вход на рынок большому количеству производителей был ограничен технической сложностью сканеров и, как следствие, их высокой стоимостью, а также высокой ценой ПО из-за монопольного положения Iridian на рынке. Эти факторы позволяли развиваться в области распознавания радужной оболочки только крупным компаниям, скорее всего уже занимающимся производством некоторых компонентов, пригодных для системы идентификации (оптика высокого разрешения, миниатюрные камеры с инфракрасной подсветкой и т.п.). Примерами таких компаний могут быть LG Electronics, Panasonic, OKI. Они заключили договор с Iridian Technologies, и в результате совместной работы появились следующие системы идентификации: Iris Access 2200, BM-ET500, OKI IrisPass. В дальнейшем возникли

	Устойчивость к подделке	Устойчивость к окружающей среде	Простота использования	Стоимость	Скорость	Стабильность признака во времени
Рад. оболочка	10	9	8	7	10	10
Дактилоскопия	6	10	9	10	10	9
Лицо 2D/3D	4/9	6/8	6/10	10/5	10/7	8/10
Вены руки	10	7	9	7	8	7
Сетчатка	10	10	6	3	6	9

Таб. 10.

усовершенствованные модели систем, благодаря техническим возможностям данных компаний самостоятельно развиваться в этой области. Следует сказать, что вышеперечисленные компании разработали также собственное ПО, но в итоге в готовой системе отдают предпочтение программному обеспечению Iridian Technologies.

На российском рынке преобладает продукция зарубежных компаний. Тем не менее, развитие технологий в последние годы позволит производителям провести быструю разработку системы. Так, производитель может использовать в ПО системы стороннюю библиотеку распознавания радужной оболочки. В России это EyeR SDK. Сканер можно собрать из доступных компонентов: камера, ИК-подсветка, управляемый объектив и различные управляющие элементы. В этом случае общая стоимость системы значительно снизится по отношению к уже готовой. Сложнее, но выгоднее при больших объемах продаж или для получения дополнительных конкурентных преимуществ разработать электронику сканера радужной оболочки.

Рисунок вен ладони

Распознавание по рисунку вен руки является довольно новой технологией, и в связи с этим ее удельный вес на мировом рынке невелик и составляет около 3%. Однако к данному методу проявляется все больший интерес. Дело в том, что, являясь довольно точным, этот метод не требует столь дорогого оборудования, как, например, методы распознавания по геометрии лица или радужной оболочке. Сейчас многие компании ведут разработки в данной сфере. Так, например, по заказу английской компании TDSi было разработано ПО для биометрического считывателя вен ладони PalmVein, представленного компанией Fujitsu. Сам сканер был разработан компанией Fujitsu в первую очередь для борьбы с финансовыми махинациями в Японии.

Также в сфере идентификации по рисунку вен работают следующие компании Veid Pte. Ltd. (scanner, software), Hitachi VeinID (scanners).

В России компаний, занимающихся данной технологией, авторам не известно.

Сетчатка глаза

Что касается сетчатки глаза, на данный момент практически не видно никаких сдвигов в сторону развития данной технологии. Несколько лет назад компания EyeDentify выпустила терминал Icam 2001. На российском рынке существовало несколько модификаций этого устройства.

Также была представлена система Ibox 10 (оптический блок в ней представлял собой передвинуемую камеру). Стоимость такой системы колебалась в пределах 7–10 тыс. долларов. Безусловно, такая цена не способствовала ее распространению на рынке. Стоимость новой системы — ICAM2001 — существенно снизилась, однако на российском рынке данные устройства так и не утвердились. Возможно, это связано с некими неудобствами, возникающими при сканировании, а также с чисто психологическими трудностями человека и боязнью перед сканированием сетчатки.

Высокая стоимость, технические сложности и неудобство в использовании — все эти факторы значительно замедлили скорость развития метода.

Выводы

Даже в классе статических систем биометрии имеется большой выбор систем. Какую из них выбрать? Все зависит от требований к системе безопасности. Самыми статистически надежными и устойчивыми к подделке системами доступа являются системы допуска по радужной оболочке и по сетчатке глаза. На первые из них существует более широкий рынок предложений. Но и это не предел. Системы биометрической идентификации можно комбинировать, достигая астрономических точностей. Самыми дешевыми и простыми в использовании, но обладающими хорошей статистикой, являются системы допуска по пальцам. Допуск по 2D-лицу удобен и дешев, но имеет ограниченную область применения из-за плохих статистических показателей.

Рассмотрим характеристики, которые будет иметь каждая из систем: устойчивость к подделке, устойчивость к окружающей среде, простота использования, стоимость, скорость, стабильность биометрического признака во времени (Таб. 10). Расставим оценки от 1 до 10 в каждой графе. Чем ближе оценка к 10, тем лучше система в этом отношении.

Также рассмотрим соотношение FAR и FRR для этих систем. Это соотношение определяет эффективность системы и широту ее использования.

	0.1%	0.01%	0.001%	0.0001%	0.00001%
Рад. оболочка	0,065%	0,07%	0,115%	0,15%	0,16%
Дактилоскопия	0,3%	0,4%	0,6%	0,9%	–
Лицо 2D/3D	2,5%(2D)	5%(2D) ~0,1%(3D)	6%(2D)	9%(2D)	–
Вены руки	Нет достоверных данных				
Сетчатка	Нет достоверных данных				

Таб. 11.

Стоит помнить, что для радужной оболочки можно увеличить точность системы практически квадратично, без потерь для времени, если усложнить систему, сделав ее на два глаза. Для дактилоскопического метода — путем комбинирования нескольких пальцев и распознаванию по венам, путем комбинирования двух рук, но такое улучшение возможно только при увеличении времени, затрачиваемого при работе с человеком.

Обобщив результаты для методов, можно сказать, что для средних и больших объектов, а также для объектов с максимальным требованием в безопасности, следует использовать радужную оболочку в качестве биометрического доступа и, возможно, распознавание по венам рук. Для объектов с количеством персонала до нескольких сотен человек оптимальным будет доступ по отпечаткам пальцев. Системы распознавания по 2D-изображению лица весьма специфические. Они могут потребоваться в случаях, когда распознавание требует отсутствия физического контакта, но поставить систему контроля по радужной оболочке невозможно. Например, при необходимости идентификации человека без его участия, скрытой камерой, или камерой наружного обнаружения, но возможно это лишь при малом количестве субъектов в базе и небольшом потоке людей, снимаемых камерой.

Подобная информация на сайте www.eyer-sdk.ru