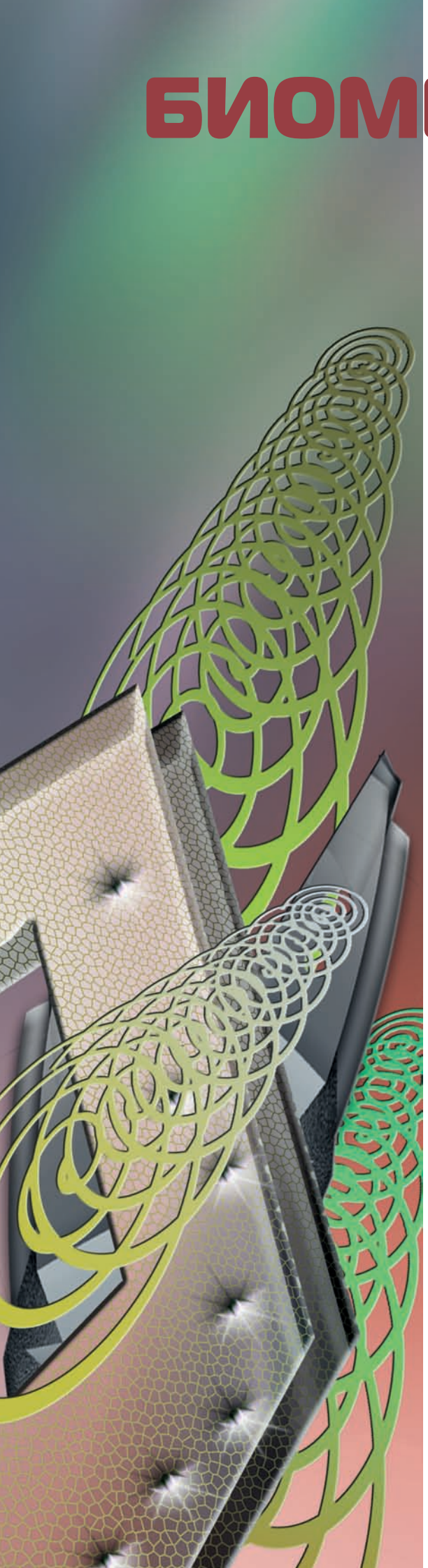


БИОМЕТРИЯ – ДЕНЬ СЕГОДНЯШНИЙ

С. Чакчир, В. Литвиненко
отделение биометрических технологий BIOCODE
ООО «НПП «Лазерные системы»

4,6 млрд долларов США. Пятикратный рост. Это прогнозы экспертов для рынка биометрических технологий на 2008 год. Что касается российского рынка, доля систем с биометрической идентификацией составит более 50%, а биометрия станет самым интенсивно развивающимся сегментом рынка безопасности. Прогнозы экспертов выглядят оптимистично. Однако результаты деятельности разработчиков создают уверенность в этих данных.

11 сентября и глобальная проблема международного терроризма – это не только новые международные отношения, это необходимость новых решений в области безопасности. И один из ее важнейших аспектов – установление подлинности личности, а подобные решения лежат в области биометрических технологий.

Цель любой системы контроля доступа – пропустить авторизованных посетителей. Система, основанная на использовании карточек, позволяет контролировать доступ, однако не определяет личность человека, который предоставляет карточку.

Биометрия идентифицирует человека по уникальным характеристикам: размеру и форме руки, отпечатку пальца, лицу или радужной оболочке глаза. Априори эти характеристики неповторимы. Они не меняются со временем и составляют нашу уникальность.

Биометрия сегодня – это инвестиции и активный рост рынка, все новые и новые разработки, совершенствующиеся системы и технологии. На 2006 год технологии, применяемые для идентификации личности пользователей, распределяются следующим образом (рис. 1):

– идентификация по отпечатку пальца – 71%;
– геометрии руки – 8%;
– радужной оболочке – 6%;
– сетчатке, радужной оболочке глаза – 6%;
– рисунку вен – 5%;
– геометрии лица – 6%;
– голосу – 4%.

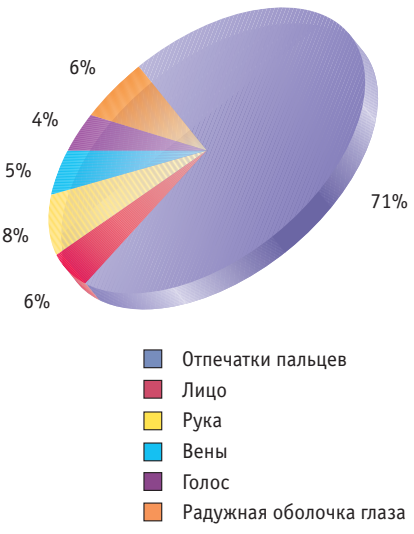
Это информация по рынку биометрического контроля доступа в России, что в целом повторяет мировые тенденции. В мире доля дактилоскопии также превышает популярность остальных имеющихся и разработанных технологий. По данным International Biometric Group, доля систем распознавания по отпечаткам пальцев составляет 52% от всех используемых в мире биометрических систем, и по прогнозам объем продаж таких систем с 2003 года (500 млн долл.) каждый год удваивается.

Популярность дактилоскопии можно объяснить длинным путем развития. Поэтому идентификация по отпечатку пальца – один из наиболее изученных и разработанных алгоритмов идентификации. В XIV веке в Персии отпечатками пальцев «подписывали» различные государственные документы, с конца XIX века уникальность рисунка человеческого пальца взяла на вооружение криминалистика. Кроме того, изученность метода и история его применения, добавили технологии еще одно существенное преимущество. И для массового российского рынка оно, безусловно, неоспоримо. Это доступная цена. Данный фактор играет не последнюю роль при выборе различных методов и средств создания систем безопасности, а применение других технологий часто усложняет эксплуатацию систем и существенно повышает их стоимость.

Биометрия – это не только технологии, защищающие сверхсекретные военные объекты и доступ к государственным тайнам. Идентификация личности – это удобство для пользователя, позволяющее не носить с собой дополнительные ключи от рабочего кабинета, банковской ячейки или кабинки в спортивном клубе.

Дополнительные преимущество дактилоскопии – в простоте регистрации и использования. Уровень ошибок и скорость обработки и сравнения информации совершенствуются феноменальными темпами. В результате достигнуты параметры: 60 тыс. отпечатков в секунду, небольшой

Рис. 1. Технологии идентификации, 2006 год.



формат хранения данных, отсутствие психологических барьеров, различные методы считывания информации.

Старейшей технологией сканирования отпечатка пальца является оптическая. Сканирование отпечатка пальца мини-камерами на ПЗС или КМОП-чипе позволило существенно уменьшить стоимость систем идентификации.

Кроме того, распространены емкостные сканеры отпечатка пальца, которые изготавливают на кремниевой пластине, содержащей область микроконденсаторов (рис. 2). Обычно всю кремниевую область защищает специально разработанное покрытие – твердый и стойкий слой, способный уберечь кремниевые схемы, но настолько тонкий, что позволяет пальцу максимально приблизиться к ним. Недостатком может быть вероятность повреждения датчика электростатическим разрядом. Чтобы его отвести, применяются дополнительные меры, которые в современных датчиках настолько совершенны, что сканеры отпечатка пальца способны противостоять разрядам свыше 15 кВ.

Новой является технология использования электромагнитного поля. Электромагнитный сигнал, излучаемый датчиком, следует по рисунку пальца и, фиксируя изменения этого сигнала, составляет образ отпечатка. Такой принцип приводит к хорошим результатам при распознавании бледных или стершихся отпечатков.

Еще одна перспективная технология – ультразвуковая: трехмерный ультразвуковой сканер измеряет пересеченную поверхность пальца своего рода радаром. Преимуществами этого метода являются качество считывания и удобство – отпечаток легко считывается даже через резиновые или пластиковые перчатки хирурга. Главный недостаток ультразвуковой технологии – ее высокая стоимость и длительное время сканирования.

Для оценки качества работы алгоритма сравнения отпечатков пальцев существуют характеристики, по которым легко можно получить количественные показатели, определяющие надежность создаваемых систем. Эти характеристики обусловлены наличием ошибок первого и второго рода.

Ошибка первого рода появляется при сравнениях «свой к своему», когда «свой» признается системой «чужим». Обозначается как FRR (False Rejection Rate) – вероятность ошибки первого рода, т.е. вероятность отказа «своему». При этом существует обратная характеристика ошибки первого рода: GAR (Genuine Acceptance Rate) = 1 – FRR, вероятность пропуска «своего».

Ошибка второго рода появляется при сравнениях «чужой к чужому», когда «чужой» признается «своим». Обозначается как FAR (False Acceptance Rate) – вероятность ошибки второго рода, т.е. вероятность пропуска «чужого». Для комплексной оценки алгоритма существует параметр EER (Equal Error Rate) – уровень ошибок биометрической системы доступа, при котором FAR и FRR равны.

Дактилоскопическая идентификация имеет свои недостатки. Так, приблизительно у 1-2% людей отпечатки пальцев имеют плохое качество. Люди, занятые физическим трудом, получают во время работы многочисленные мелкие травмы, верхний слой кожи рук может быть поврежден, что создает большие трудности при сравнении отпечатков. Отпечаток может также деформироваться при большой влажности и под воздействием ряда других внешних факторов. В связи с этим выполнение жестких требований по производительности работы алгоритмов, характерных для гражданских приложений, все еще является достаточно серьезной проблемой.

Идентификация по геометрии руки

Технологии идентификации пользователей по очертаниям ладоней рук доступны на протяжении уже 20 лет. При применении данного метода за 1-2 секунды оценивается более 90 различных характеристик, включая размеры самой ладони (три измерения), длину и ширину пальцев, очертания суставов и т.п. В настоящее время идентификация пользователей по геометрии руки используется в законодательных органах, международных аэропортах, больницах и т.д. Преимущества идентификации по геометрии ладони сравнимы с плюсами идентификации по отпечатку пальца в вопросе надежности, хотя устройство для считывания отпечатков ладоней занимает больше места.

Технология использует цифровую камеру с разрешением 32 тыс. пикселей для записи формы руки в трехмерном изображении, полученном от сканера. Сканер не обращает внимания на детали верхнего покрова руки, такие как царапины, шрамы, грязь и т.п.

Способ сравнения – верификация или идентификация – идентичен другим технологиям, прежде всего, дактилоскопическим.

Процесс регистрации занимает около 30 секунд. Пользователь помещает правую руку на считывающее устройство три раза, процессор и программа преобразовывают изображение в 9-байтный математический отпечаток, который является собирательным образом трех представленных изображений.

Специалисты отмечают, что для технологии идентификации по форме руки характерен достаточно низкий уровень ошибок первого рода, при высоком уровне защиты от неавторизованных пользователей. В среднем уровень ошибок данных систем оценивается специалистами как 0,2 %, что значительно выше, чем вероятность ошибки системы, основанной на технологиях идентификации по отпечаткам пальцев.

Данная технология часто используется на таможенном и миграционном контроле и позволяет сократить очереди среди часто летающих пассажиров в международных аэропортах Лос-Анджелеса, Майами, Нью-Джерси, Нью-Йорка, Вашингтона, Сан-Франциско, Торонто и Ванкувера. Авторизованные пассажиры после регистрации в системе получают карточку с магнитной полосой с закодированной информацией о форме руки. Вместо прохождения паспортного контроля пассажиры подносят карточку и прикладывают руку к считывающему устройству.

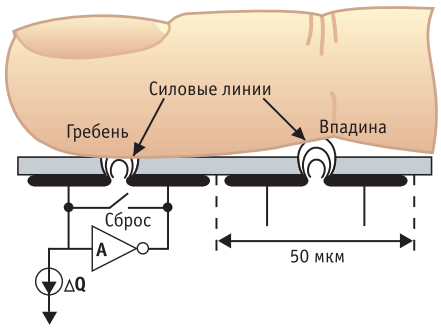


Рис. 2. Емкостное сканирование

Сетчатка глаза

Метод идентификации по сетчатке глаза получил практическое применение в середине 50-х годов XX века: было доказано, что рисунок кровеносных сосудов сетчатки не совпадает даже у близнецов. Для сканирования сетчатки используется инфракрасное излучение низкой интенсивности, направленное через зрачок к кровеносным сосудам на задней стенке глаза. Информация о нескольких сотнях характерных точках сохраняется в кодированном файле.

К недостаткам подобных систем следует в первую очередь отнести психологический фактор. Световой пучок, направляемый в глаз в процессе сканирования, не вызывает приятных эмоций. К тому же необходимо следить за положением глаза относительно отверстия, поскольку подобные системы чувствительны к неправильной ориентации сетчатки.

Для регистрации достаточно смотреть в глазок камеры менее минуты. За это время система успевает подсветить сетчатку и получить отраженный сигнал. Благодаря почти нулевому проценту ошибок второго рода и одному из самых низких показателей ошибок первого, сканеры для сетчатки глаза получили широкое распространение при организации доступа к сверхсекретным системам.

Идентификация по радужной оболочки глаза

Этот способ идентификации основан на анализе цветной радужной оболочки глаза, окружающей зрачок. Радужная оболочка человеческого глаза не меняется практически в течение всей его жизни, невосприимчива к загрязнению и ранам. Заметим также, что радужки правого и левого глаза по рисунку существенно различаются. Образцы радужных оболо-

чек становятся доступными с помощью видеосистем. Подобные системы смогут идентифицировать человека, даже если он будет в очках или с контактными линзами.

Различают активные и пассивные системы распознавания. В системах первого типа пользователь должен сам настроить камеру, передвигая ее для более точной наводки. Пассивные системы проще и удобнее в использовании, поскольку камера в них настраивается автоматически.

Преимущество современных сканеров для радужной оболочки состоит в том, что они не требуют, чтобы пользователь сосредоточился на цели, потому что образец пятен на радужной оболочке находится на поверхности глаза. Фактически видеоизображение глаза можно отсканировать даже на расстоянии менее метра, а поиск и сравнение снимка радужки с данными, хранящимися в базе данных, занимают лишь пару секунд.

Основной недостаток данной технологии состоит также в психологическом барьере. Процедура прохождения, как регистрации пользователей, так и идентификации при прохождении контроля, у большинства вызывает отрицательные эмоции.

Идентификация по рисунку вен руки

Это технологии XXI века. Первые системы были представлены в 2004 году. Производители заявляют следующий уровень ошибок:

– не могут опознать 0,01%;
– ложно идентифицируют 0,00008%.

С помощь инфракрасной камеры считывается рисунок вен на лицевой стороне ладони или кисти руки. Восстановленный гемоглобин, который доставляет кислород к клеткам нашего организма по венам, поглощает эти лучи, сокращая тем самым степень отражения и отображая вены в виде чёрного орнамента. Полученная картинка обрабатывается и по схеме расположения вен формируется цифровая свертка. Необходимо также отметить, что качество считываемой информации не зависит от расстояния между поверхностью устройства и ладонью или от сканирования лишь участка ладони. Идентификация человека занимает полсекунды.

К преимуществам систем распознавания по рисунку вен можно отнести уникальное расположение вен каждого человека, а также бесконтактность идентификации и тот факт, что система имеет высокую степень распознавания при наличии небольших ран и естественных искажений сухой или влажной кожи.

Поскольку рисунок вен каждого человека представляет собой многообразие различных свойств и признаков и очень сложно подделать идентификацию, следовательно, гарантируется высокая степень безопасности. Рисунок вен на ладони человека не будет изменяться в течение всей его жизни, и предварительная регистрация может производиться, когда ребенок находится в утробе матери.

Геометрия лица

Техническая реализация распространенного в обычной жизни способа распознавания личности – по лицу – представляет собой сложную задачу. Среди множества применяемых сегодня биометрических технологий идентификация по лицу вызывает особый интерес. Это связано с тем, что день ото дня мы узнаем друг друга в лицо. Еще одним преимуществом технологии распознавания по лицу является возможность бесконтактного получения биометрических данных – регистрация и идентификация проводятся дистанционно с помощью оптических приборов.

В основу метода автоматической идентификации личности по геометрии лица (трехмерное распознавание) положен постулат о том, что форма черепа каждого человека индивидуальна. Так как получение точной модели черепа – задача более чем трудноразрешимая, его форму восстанавливают по поверхности лица. На лице существуют определенные точки, учитывая пространственные координаты которых, можно вычислить координаты точек на черепе, которые и будут участвовать в идентификации. Причем количество подобных точек, необходимое для уверенной идентификации, невелико – несколько десятков. Сложность заключается в том, что измерения необходимо выполнять с очень высокой точностью, а задача восстановления изображения лица и формы черепа требует довольно много процессорного времени. Кроме того, грамотная реализация этого метода идентификации требует дорогостоящей аппаратуры (нужны цифровая видео- или фотокамера и плата захвата видеоизображения).

Обычно камера устанавливается на расстоянии в несколько десятков сантиметров от объекта. Получив изображение, система анализирует различные параметры лица (например, расстояние между глазами и носом). Алгоритм должен учитывать возможные возрастные изменения, наличие очков, шляпы или бороды, изменения прически и т.п. Для этой цели обычно используется сканирование лица в инфракрасном диапазоне.

К преимуществам данной технологии можно также отнести: нечувствительность к условиям освещения (приборы могут работать как при солнечном свете, так и в помещении, и при полной темноте); сложность подделки – для того, чтобы «обмануть» систему, придется изготовить точную копию лица человека, причем сделать это с субмиллиметровой точностью – именно с такой точностью сканирует лицо трехмерный сканер. Кроме того, живая кожа человека имеет уникальные свойство рассеивания инфракрасного света. Замена ее другим материалом будет обнаружена.

Комплексные задачи по созданию достаточно точных технологий идентификации по геометрии лица были решены недавно. Система, основанная на данном принципе распознавания, позволяет в реальном времени сканировать поверхность лица, выделять модель твердых тканей головы (черепа) и проводить сравнение с заранее сохраненными моделями. предполагается, что на качество распознавания практически не влияют возрастные и естественные изменения внешности (усы и борода), очки, при условии, что это не темные очки и они не имеют массивной оправы. В связи с тем, что задачи, стоящие перед идентификацией по лицу, решены недавно, алгоритм идентификации разработан недостаточно, кроме того, не хватает данных по практическому применению этих систем. Поэтому, несмотря на утверждения производителей, эксперты оценивают возможность ошибок системы при идентификации пользователей до 5%.

Идентификация по голосу

Распознавание голоса может использоваться для диктовки текста компьютеру или проговаривания (таких, как открытие определенных программ, сворачивание меню, сохранение данных, или, например, управление «умным домом»).

Первоначальные технологии распознавания голоса распознавали слова только в случае их раздельного произнесения. Машине необходимо было определить, где кончается одно слово и начинается другое. Такие технологии распознавания голоса все еще встречаются для управления компьютерными системами. Современные применения данной технологии позволяют пользователю быстро и слитно произносить текст. Новые системы могут распознать до160 слов в минуту, позволяя преобразовывать непрерывную речь в узнаваемый текст и форматировать его.

Различия голосов у разных людей обусловлены физиологическими характеристиками, такими как голосовые связки, трахеи, носовой проход, тем, как язык двигается во рту, и тем, как извлекаются звуки и т.д. Комбинация этих характеристик анализируется и представляется уникальной для каждого человека. Голос является уникальной биометрической характеристикой человека и может использоваться для подтверждения его личности.

Основные задачи распознавание речи связаны с тем, что было сказано, и с тем, кто именно говорит. Системы голосовой идентификации не зависят от какого-либо языка или словаря. Человек может сказать что угодно и на каком угодно языке, благодаря чему эти системы можно назвать идеальными для международного использования.

Идентификация по голосу происходит по следующей схеме: система сравнивает образец голоса, представленного в цифровой форме, с так называемым «голосовым отпечатком» (цифровое изображение уникальных характеристик голоса), хранящимся в базе данных.

Что касается занесения в базу, то процесс занесения данных занимает несколько минут. Система предлагает ответить на несколько простых вопросов, например ваше имя, отчество, фамилия или дата рождения. Ответы становятся идентификационными фразами, которые позднее будут использоваться для идентификации человека. Важно, чтобы ответ был хорошо знаком человеку и он смог его воспроизвести в любую минуту. Для каждого вопроса пользователь произносит свой ответ четыре раза. Ответ должен состоять, как минимум, из трех слогов и длиться больше секунды. Для создания «голосового отпечатка» записанные ответы накладываются друг на друга.

Безусловно, успех голосовой идентификации зависит от неизменного, устойчивого образца. Для голосовой идентификации неизменный, устойчивый образец – это значит говорить спокойно, в своей обычной манере. Также пользователи должны понимать, что жевательная резинка, одышка, а также алкоголь негативно отражаются на голосе.

В случае обычной простуды система, вероятнее всего, вас узнает, так как при простуде не все характеристики вашего голоса пострадают. А вот более серьезные заболевания горла (например, ларингит) вызовут проблему с прохождением идентификации.

Как недостаток идентификации по голосу стоит отметить также большой размер хранящихся «голосовых отпечатков». В зависимости от длины устойчивого образца, системе понадобится от 15 до 40 Кб для хранения одного «голосового отпечатка».

Применения систем голосовой идентификации уже можно встретить по всему миру. Компании радио- и телевещания используют системы голосовой идентификации для обеспечения безопасности данных, передаваемых на большие расстояния.

Описанные технологии – основные из применяемых сегодня. Перспективность биометрических технологий как в целом, так и отдельно взятых методов, несомненна. Напомним, что, по прогнозам экспертов, прибыль участников мирового рынка биометрии оценивается в 5 млрд долларов. Что касается, оценок специалистов на самом российском рынке систем безопасности, то в силу складывающихся тенденций рынка, приоритетность разработок и инвестиций в продвижение подобных технологий оценена.

Сегодня аналитики прогнозируют серьезное развитие всех трех направлений, в частности – систем гражданской идентификации в связи со стартом проекта «Российский биометрический паспорт» в Калининграде и Калининградской области. Это послужило мощным импульсом к развитию биометрической индустрии в России – снижается стоимость устройств, растет надежность, повышается уровень зрелости общества, необходимый для массового принятия технологии.

Наиболее перспективными направлениями в настоящее время являются технологии идентификации по отпечаткам пальца и бесконтактная биометрия, в первую очередь – технологии трехмерного распознавания лица. Кроме того, широкими возможностями обладает интеграций различных технологий контроля доступа для повышения уровня безопасности объектов.

Несколько слов о возможностях обмануть системы. Вопреки бытующему мнению о том, что «обмануть» сканер отпечатков пальцев несложно, следует отметить, что в настоящее время ведущим производителям устройств сканирования отпечатков пальцев удалось создать комбинацию аппаратного и программного обеспечения, устойчивую к подделкам и муляжам. А для систем биометрической идентификации на основе радужной оболочки глаза стоимость создания «муляжа» сопоставима со стоимостью совокупного владения системой.

Небольшое резюме. Самыми доступными и самыми распространенными на сегодня и на ближайшие 5 лет остаются системы идентификации по отпечатку пальца, а самые точные на настоящий момент – технологии идентификации по сетчатке глаза. Среди мировых производителей, занимающихся технологией идентификации по сетчатке глаза, среди российских компаний наибольшим уважением пользуются системы Panasonic. А ведущим участником российского рынка систем дактилоскопической идентификации является научно-производственное предприятие «Лазерные системы», которое представляет торговую марку BIOCODE.