Смотри в глаза!

Как работает биометрическая идентификация

Биометрические системы все чаще используются для организации контроля доступа не только в организациях, но даже и на бытовом уровне. Но как же они устроены, по каким принципам работают и действительно ли так надежны, как принято считать?

Впустить или не впустить, запретить или разрешить? Во все времена и в любых системах безопасности вопрос верной идентификации человека стоял достаточно остро. Вместе с тем этот аспект является и одной из наиболее уязвимых точек системы условного доступа. Если ключ подобран — замки бесполезны. Поэтому системе паролей и условных знаков всегда уделялось очень большое значение на всех этапах создания систем безопасности. Но как определить, что человек, который просит доступа — именно тот, за кого себя выдает? Ведь пароль, ключ или, скажем, карту доступа можно выкрасть, а пропуск или удостоверение подделать.

Долгое время единственным надежным средством точной идентификации являлось (и зачастую остается) привлечение к этой задаче человека — охранника, вахтера, пограничника, который бы мог проверить соответствие документа или ключа и человека, который его предъявляет. Но в наш век компьютерных технологий такой метод уже становится анахронизмом, да и надежность его, в общем, все же недостаточная — человеческий фактор неизбежно оказывает сильное влияние. Поэтому задачу точного определения объекта возложили на электронные системы аутентификации, использующие уникальные биометрические признаки человека. Хотя такие решения являются относительно новыми и все еще обладают целым рядом недостатков, их эффективность, а также востребованность на рынке растет буквально с каждым днем, и тому есть немало веских причин.

Встретить и узнать

Ни один из методов условного доступа сам по себе не является абсолютно надежным. Гораздо эффективнее многофакторная аутентификация. Желательно с использованием каких-то уникальных признаков человека, на роль которых идеально подходят различные физиологические особенности — лицо, отпечатки пальцев, рисунок радужной оболочки или сетчатки глаза — практически идеальные кандидаты, но есть и множество других (о которых поговорим в отдельном разделе). Собственно, классическая двухфакторная идентификация на основе биометрических данных известна каждому, кто хоть раз проходил паспортный контроль на границе — документ является первичным ключом, на основе которого контролер определяет и сверяет личность человека, а также его права доступа, соответственно с информацией в базе данных. Но это полуавтоматизированная система, которая не обходится без участия оператора. Мы же будем говорить о полностью самостоятельных решениях.

Для начала следует пояснить два ключевых термина, которые часто используются при описании работы систем контроля доступа (СКД) — это ***идентификация*** и ***верификация*** (или аутентификация). Первое понятие подразумевает, что подтверждение личности осуществляется только на основе какого-либо одного ключевого признака — это может быть, например, смарт-карта, брелок, чип или в случае биометрических методов отпечаток пальца. Верификация означает более глубокую степень обеспечения безопасности и означает, что объект не только идентифицирован, но и безошибочно узнан — т.е. документ или отпечаток пальца действительно принадлежат предъявившему их лицу с соответствующими правами доступа. Естественно, идентификация является более быстрым и менее дорогим методом, поэтому ею в большинстве случаев и ограничиваются, особенно на коммерческих предприятиях (т.е. в данном случае идентификация и верификация являются синонимами). Но на ответственных объектах используются многофакторные СКД, которые хотя и дороже, но гораздо более надежны.

Предъявите тело

К наиболее распространенным сегодня методам биометрического контроля доступа относится идентификация по отпечаткам пальцев, голосу, рисунку радужной оболочки или сетчатки глаза и лицу в целом. В последнее время появляются и другие подходы, использующие в качестве модели поведенческие факторы, мелкую моторику лица, походку и даже движение губ при произнесении условного пароля. При этом контроль может быть контактным (скажем, дактилоскопия) либо бесконтактным (например, современная видеокамера, оснащенная средствами видеоаналитики, может «узнать» человека на значительном расстоянии, даже в толпе).

Самым распространенным на сегодня методом остается идентификация по отпечаткам пальцев, доля продаж систем этого вида, по данным исследовательской компании IHS, составляет около 90% всего рынка биометрических СКД. Возможно, этот показатель еще больше. Основная причина такого положения дел очевидна и заключается она в цене — дактилоскопический терминал доступа стоит сегодня $200–300, в то время как, например, профессиональный сканер радужной оболочки или сетчатки глаза обойдется в десять раз дороже. При этом общий объем мирового рынка биометрических СКД все еще относительно невелик. Например, компания Tractica определяет его в $2,4 млрд по итогам 2016 года, в то же время Frost & Sullivan сообщала, что этот сегмент достиг $4,49 млрд еще в 2010 году, а согласно оценкам J'son & Partners Consulting, объем мирового рынка биометрических систем по итогам прошлого года вообще составил $14 млрд.

Очевидно, компании используют различные определения для того, что же включать в состав биометрических СКД — скажем, бытовые дактилоскопические сканеры, которые используются в ноутбуках, смартфонах, ручках дверей и даже «умных» чемоданов, вполне могут оказывать существенное влияние на объем показателей. Однако все исследователи сходятся в одном — рынок биометрических систем постоянно растет, причем достаточно быстро — на десятки процентов в год. Так, уже упомянутая компания J'son & Partners Consulting рассчитывает, что к 2022 году этот рынок достигнет отметки в $40 млрд. Поводом для столь обнадеживающих прогнозов является мощное участие госсектора. В частности, все больше стран переходят на биометрические паспорта и идентификационные карточки. Например, компания Acuity Research сообщает, что в 2015 году таких документов в мире насчитывалось около 600 млн, а к концу 2018-го будет уже 740 млн.

К примеру, в Индии сейчас реализуется проект под названием AADHAAR, в рамках которого собираются биометрические данные (отпечатки пальцев и фотографии радужных оболочек глаз) всех резидентов государства. По состоянию на август 2017 года в базе данных хранилась информация об 1,2 млрд человек — для каждого одно фото лица, два снимка радужной оболочки и десять отпечатков. На сегодняшний день — это крупнейшая биометрическая база данных в мире.

В последнее время все более популярным методом становится идентификация по голосу, главным образом из-за стоимости реализации подобных систем, которая ощутимо ниже всех остальных. Ведь если для получения отпечатка пальца требуется специальный достаточно сложный и дорогой сканер, то в случае идентификации по голосу — только качественный микрофон.

«Интеллектуальная» же часть системы в обоих случаях представлена специальным ПО, работающим на сервере. Почему же распознавание по голосу становится массовым явлением, популярным в корпоративных СКД лишь сейчас? Дело в том, что до недавнего времени надежность подобного метода идентификации была под вопросом, поскольку слишком много факторов могли вносить существенные искажения. Скажем, фоновый шум или банальная простуда могут изменить голос до неузнаваемости. Тем не менее новые алгоритмы обработки звуков постепенно исключают эти моменты и делают решения все более надежными.

ПАЛЬЦЫ-УНИКАЛЬЦЫ?

Тот факт, что отпечатки пальцев являются уникальным признаком человека, был подмечен достаточно давно. Еще в середине 14-го века китайские купцы «подписывали» торговые договоры, приложив к ним свой большой палец, покрытый черной тушью. Впоследствии этот метод взяли на вооружение англичане, платившие жалование индийским солдатам – последние были для колонизаторов на одно лицо, да и писать, как правило, не умели. Индийцы быстро смекнули, что к чему, и норовили получить выплаты по несколько раз, называясь разными именами. Но отпечаток пальца и здесь стал уникальным идентификатором. Гипотезу о том, что нет двух людей с одинаковым папиллярным рисунком, высказал в конце 19-го века Фрэнсис Гальтон, двоюродный брат Чарльза Дарвина. Точнее, он рассчитал, что вероятность совпадения составляет ничтожный шанс – 1/64x109. С тех пор метод дактилоскопии (термин также введенный Гальтоном) обрел научную основу и стал использоваться в т.ч. для нужд криминалистики. Хотя справедливости ради стоит отметить, что на самом деле до сих пор не существует основательной теории, которая бы действительно доказала уникальность отпечатков пальцев. Единственным подтверждением является лишь эмпирический фактор – отсутствие фактических совпадений, что, строго говоря, не является научным подходом..

Более того, в криминалистике дактилоскопия является больше «искусством», чем обоснованным методом. Ведь совершенно точно можно сравнить лишь отпечатки пальцев, полученные в одинаковых идеальных условиях. Но на месте преступления они, как правило, фрагментарны, искажены и перекрываются другими отпечатками. Так что можно говорить лишь о частичном совпадении признаков, что существенно снижает точность идентификации и увеличивает вероятность ошибки.

Можно возразить, что, мол, сканеры отпечатка пальца также не являются дорогими, ведь они применяются даже в смартфонах отнюдь не верхнего ценового диапазона. Но здесь есть важный нюанс — сканеры, используемые в пользовательских решениях, недостаточно надежны. Для них гораздо важнее скорость отклика, чем точность определения отпечатка. Поэтому во всех системах такого рода используется очень упрощенный алгоритм, который считывает лишь часть папиллярного рисунка. Системы корпоративного уровня используют более сложные технологии и требуют уже наличия не только сканера, но и выделенного аппаратного сервера, на котором работало бы специальное программное обеспечение и хранилась актуальная база данных отпечатков.

Кстати, сложности в распознавании образов испытывают и системы охранного видеонаблюдения, особенно если они установлены таким образом, чтобы вести скрытый надзор — любое изменение освещения, смена ракурса, визуальные помехи (дождь, туман, плотный поток людей) значительно снижает эффективность распознавания. Но если идентификация осуществляется в условиях, близких к идеальным, а их можно добиться, например, в офисе, то точность определения лиц современными специализированными системами видеонаблюдения приближается к 100%.

Отметим, что кроме госсектора, активными потребителями различных систем биометрической идентификации являются предприятия финансового сектора. Интернет-банкинг — популярнейшее направление, которое позволяет существенно расширить клиентскую базу, причем за счет вполне платежеспособной аудитории,

к которой в основном относятся пользователи смартфонов и беспроводного ШПД. Такие люди обычно не хотят усложнять себе жизнь посещением банковских отделений или запоминанием сложных паролей. Поэтому специально для них придумываются различные способы верификации для получения банковских услуг. Например, MasterCard уже позволяет подтверждать онлайн-покупки с помощью автопортрета (селфи). Такая услуга доступна во многих странах ЕС. Приходят на помощь и стандарты — новая версия протокола 3D Secure 2.0 включает методику подтверждения платежей с помощью биометрических данных — папиллярных линий, рисунка вен на ладонях и др.

Из производителей, активно занимающихся разработкой новых решений для биометрической идентификации и верификации, стоит отметить Toshiba (которая создает высокоточные математические модели лица) Intel, Samsung, Hitachi, LG, Fujitsu. Научные и прикладные разработки в этом направлении ведутся и во многих институтах с мировым именем.

Как работает биометрия — общая схема

Теперь давайте рассмотрим вопрос о том, как устроены системы биометрической идентификации, по каким принципам работают и в чем их слабые стороны. В общем случае любая система такого рода состоит из нескольких ключевых компонентов: сканера, каналов передачи данных, сервера со специальным ПО и базой данных, а также интерфейсов подключения к СКУД.

Сканер, наверное, самая характерная часть биометрической системы, с его помощью происходит снятие уникальных характеристик с объекта — будь то папиллярный узор или структура глазного дна. Устройства такого типа бывают контактные и бесконтактные, разница между которыми понятна уже из названия. Отличаются сканеры и по своему устройству. Это может быть, например, обычная камера (в случае распознавания лиц) или напротив — сложный оптический комплекс (если требуется сканировать сетчатку глаза).

Простые сканеры только лишь снимают биометрические показатели, в то время как более продвинутые модели осуществляют еще и первичную обработку взятого образца, оптимизируя его для поиска в базе данных. Например, преобразуют полную копию в условную математическую модель — индекс, который занимает значительно меньше места и, соответственно, быстрее передается по сети.

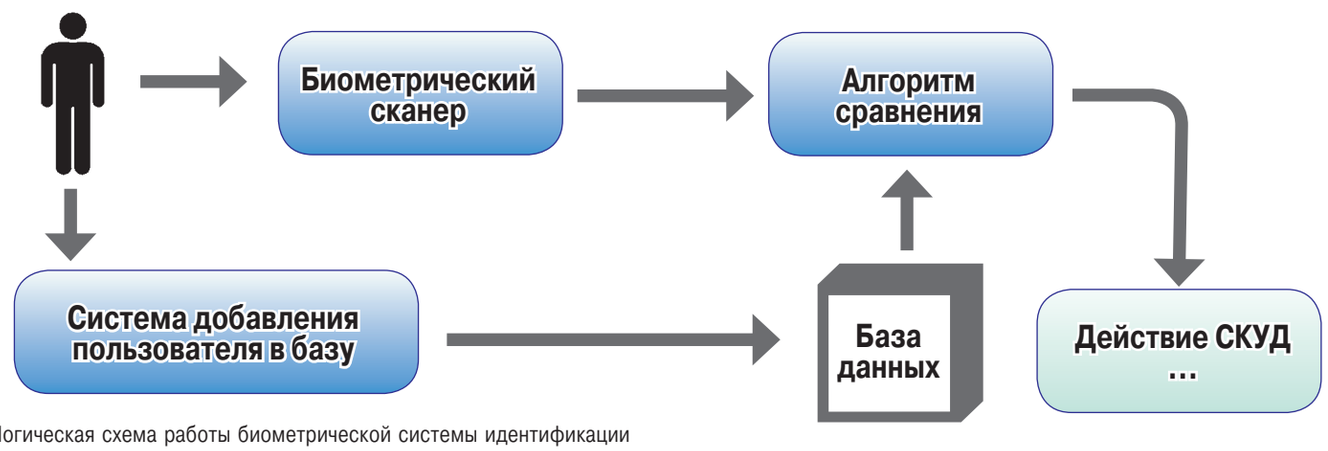
Далее полученные сведения отправляются на сервер, где, собственно, и происходит основная работа с полученным изображением или индексом, которые сравниваются с образцами, имеющимися в БД. Если совпадение найдено — выдается команда на разрешение действия, если нет — сообщение о запрете. Для этого биометрическая система должна быть интегрирована в общую СКУД организации. От качества используемых алгоритмов и математических моделей, типа идентификации и вычислительной мощности сервера существенно зависит пропускная способность биометрической системы доступа. С точки зрения безопасности слабыми местами в этой логической схеме являются каналы передачи данных, а также сама БД. Исследования, проводимые различными компаниями, показывают, что даже в экономически развитых странах вполне солидные организации нередко упускают из виду аспект шифрования биометрических данных, передающихся по сети, а защита информации в БД часто носит формальный характер. С одной стороны, это повышает скорость работы системы, но с другой, таит угрозу несанкционированного получения важной биометрической информации, которая затем может быть использована в противоправных целях.

Отметим, что в последнее время выросла популярность облачных решений, когда сервер и база данных хранятся у оператора сервиса. Но это теоретическая сторона вопроса. Теперь стоит перейти к более практическим вещам и рассмотреть, как устроены три наиболее популярных сегодня метода распознавания, формирующие более 97% мирового рынка — по отпечаткам пальцев, голосу, а также радужной оболочке и сетчатке глаза.

Сканируем отпечатки

Самые популярные на сегодняшний день сканеры предназначены для считывания папиллярного узора. Они подразделяются на три основных типа — оптические, полупроводниковые и ультразвуковые — и отличаются способом получения образца отпечатков. Наиболее распространенные из перечисленных — оптические системы, которые, в свою очередь различаются по типу используемой технологии: на отражение, на просвет или бесконтактный метод.

В сканере, работающем по принципу на отражение, внутренний источник света формирует пучок излучения, который в базовом состоянии полностью отражается от внутренней поверхности защитного покрытия сканера под определенным



Логическая схема работы биометрической системы идентификации

углом. Если приложить к такому стеклу палец, то плотность среды меняется, а с ней и форма отраженного пучка, которая, в свою очередь, сформирует на светочувствительном датчике определенное изображение, соответствующее отпечатку.

Это самый ненадежный, но при этом наиболее распространенный тип дактилоскопических сканеров — именно их, главным образом, используют для демонстрации возможных методов обмана биометрической системы, например, с помощью рисунка, распечатанного на 3D принтере, или силиконовой копии отпечатка пальца. Более надежный метод — на просвет. В этом случае используется внешний источник излучения, пучок которого проникает сквозь палец сверху. В нижней части сканера расположена волоконно-оптическая матрица, все проводники которой соединены с фотодатчиками.

Естественно количество света, проникающего сквозь различные точки пальца, будет отличаться, что позволяет сформировать схему уникального отпечатка.

В бесконтактных сканерах считывающая система отделена защитным стеклом. Поверхность пальца освещается с нескольких точек, отраженный свет попадает в специальную линзу и фокусируется на светочувствительном датчике, где происходит формирование изображения отпечатка.

Кроме оптических, существуют также полупроводниковые сканеры — емкостные, радиочастотные, реагирующие на давление. Системы первого типа используют эффект p-n-перехода, возникающий при соприкосновении выступающих линий отпечатка с элементами полупроводниковой матрицы.

В радиочастотных устройствах используется модуль, генерирующий радиосигнал, и набор специальных элементов, работающих в качестве миниатюрных антенн, которые принимают волны, отраженные от поверхности пальца. Сканер, регистрирующий на нажатие, содержит внутри группу особых пьезоэлектрических элементов, реагирующих на выпуклые линии папиллярного узора (давление которых выше, чем у впадин) и позволяющих сформировать изображение отпечатка на основе матрицы напряжений.

Еще два типа дактилоскопических датчиков основаны на использовании тепла и ультразвука. Основным компонентом термосканера являются пироэлектрические элементы, реагирующие на разницу температур, возникающую между выступающими участками папиллярного узора и воздуха, который находится во впадинах. Эти микроскопические отличия преобразуются в напряжение, которое формирует изображение рисунка. Данный подход является одним из наиболее надежных, поскольку исключает возможность использования поддельных отпечатков пальцев, выполненных на неживых поверхностях.

Ультразвуковые сканеры распознают изображение отпечатка с помощью миниатюрного эхолокатора, волны которого отражаются от выступов и впадин поверхности пальца и формируют изображение на приемнике. При этом достигается максимальная детализация и точность получаемого изображения, кроме того, ультразвуковые сканеры позволяют определить наличие пульса в пальце, а соответственно, устойчивы к использованию искусственных подделок отпечатков.

Дактилоскопический сканер

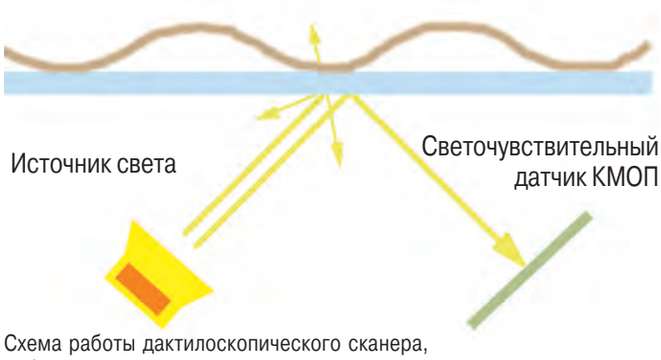


Схема работы дактилоскопического сканера, работающего по принципу на отражение

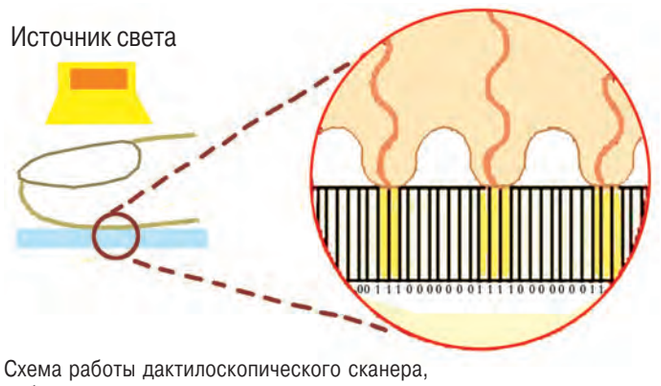


Схема работы дактилоскопического сканера, работающего по принципу на просвет

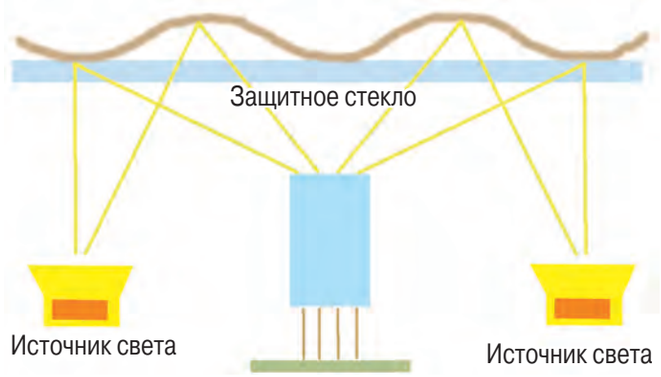
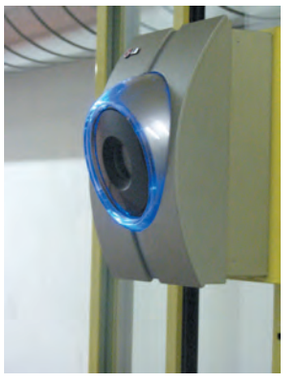


Схема работы бесконтактного дактилоскопического сканера



Профессиональный сканер сетчатки глаза

Биометрический сканер рисунка вен ладони (слева) и пальца (справа)

С глазу на глаз, или Все в твоих руках

Но рисунок пальцев во многих случаях не является надежным идентификатором. Гораздо больше информации может предоставить сканирование различных частей глаза — радужной оболочки либо сетчатки (точнее глазного дна), которые сегодня невозможно подделать. В этом процессе сканер использует направленный инфракрасный луч (он способен проникать сквозь линзы очков и не приводит к сужению зрачка), подсвечивающий рисунок радужной оболочки, который фиксируется камерой, переводится в цифровую модель, а затем сравнивается с изображениями в базе данных. Сканер сетчатки глаза работает по схожему принципу, но использует в качестве идентификатора структуру глазного дна, это значит, что такое устройство надо подносить вплотную к глазу, в отличие от считывателя радужной оболочки, способного распознавать изображение даже на расстоянии вытянутой руки.

Сканирование сетчатки является более дорогим методом, который используется главным образом в корпоративном и государственном секторах, в то время как идентификация по рисунку радужной оболочки доступна даже в некоторых новых моделях смартфонов.

Еще одним популярным методом биометрической идентификации является распознавание лиц — в двух- и трехмерной проекции. Основной подход заключается здесь в том, что человеческое лицо имеет множество уникальных признаков. При этом анализ двухмерных изображений теряет популярность, поскольку его эффективность в реальных условиях остается весьма низкой — слишком много факторов могут внести искажение, к тому же двухмерную модель лица достаточно легко подделать. Гораздо более перспективным направлением является трехмерная идентификация, в ходе которой на первом этапе создается 3D-модель лиц, заносимых в базу данных — для этого их снимают специальной камерой (или камерами) в разных ракурсах. В процессе идентификации сканер делает объемный снимок лица и сравнивает его с имеющимися образцами. Более детальное описание методов и алгоритмов в этой сфере осложнено тем, что здесь пока нет единого стандарта, и большинство производителей используют собственные подходы, ноу-хау и математические модели. Однако следует отметить, что идеал здесь все еще не достигнут. Каждая система трехмерной идентификации лиц имеет свои недостатки. Направление активно развивается, приобретает популярность, но все еще не стало массовым явлением.

Как было отмечено выше, идентификация по голосу становится все более популярной. Относительная дешевизна применения такого подхода позволяет использовать его даже в бытовых системах, а современные алгоритмы обработки звука делают его надежным средством подтверждения прав доступа даже в таких серьезных организациях, как банки. Голосовую идентификацию можно разделить на текстонезависимую (когда неважно, что говорит человек, главное получить основные характеристики его голоса) и текстозависимую (в этом случае система реагирует на произнесение конкретной фразы).

Чтобы идентификация работала эффективно, для начала создается база данных из нескольких образов голоса каждого человека, который может запросить те или иные права доступа. Для этого обычно надо произнести специальные фразы, последовательность цифр, наборы слов, которые обрабатываются сервером, преобразуются в цифровую модель и записываются в базу данных. В случае запроса доступа человек также должен предоставить образец речи (сказать ключевую фразу, произнести пароль, просто назвать себя и т.д.), который сравнивается с моделями, находящимися в БД. Если найдено соответствие — доступ разрешается. При этом реальный голос далеко не всегда совпадает с образцами, поэтому в большинстве систем применяется т.н. порог доверия, который выражается в процентах и отражает степень соответствия идеальной модели (в каждом случае он устанавливается исходя из конкретных условий проекта и степени ответственности).

Перспективным бесконтактным методом биометрической идентификации является использование венозного рисунка кистей рук. В этом случае используется специальная камера, работающая в инфракрасном спектре и оснащенная ИК-подсветкой. Гемоглобин крови поглощает ИК-излучение, в результате чего отчетливо виден венозный рисунок, изображение которого фиксируется камерой, преобразуется в цифровую модель и сравнивается с изображениями из БД. Причем неважно, какая поверхность руки облучается — внешняя или внутренняя, уникальны обе.

Существует также немало других способов биометрической идентификации, но они пока что не столь популярны, как вышеперечисленные. В целом же технологии данного направления развиваются стремительно, рынок растет тоже очень быстро. Еще совсем недавно такие решения были доступны лишь узкому кругу корпоративных и государственных заказчиков. Но сегодня они активно выходят на массовый рынок и становятся повсеместным явлением. Собственно этот процесс знаменует собой очередную веху в развитии информационных технологий и систем безопасности, которые становятся все более надежными и персонифицированными.

Игорь КИРИЛЛОВ, СиБ