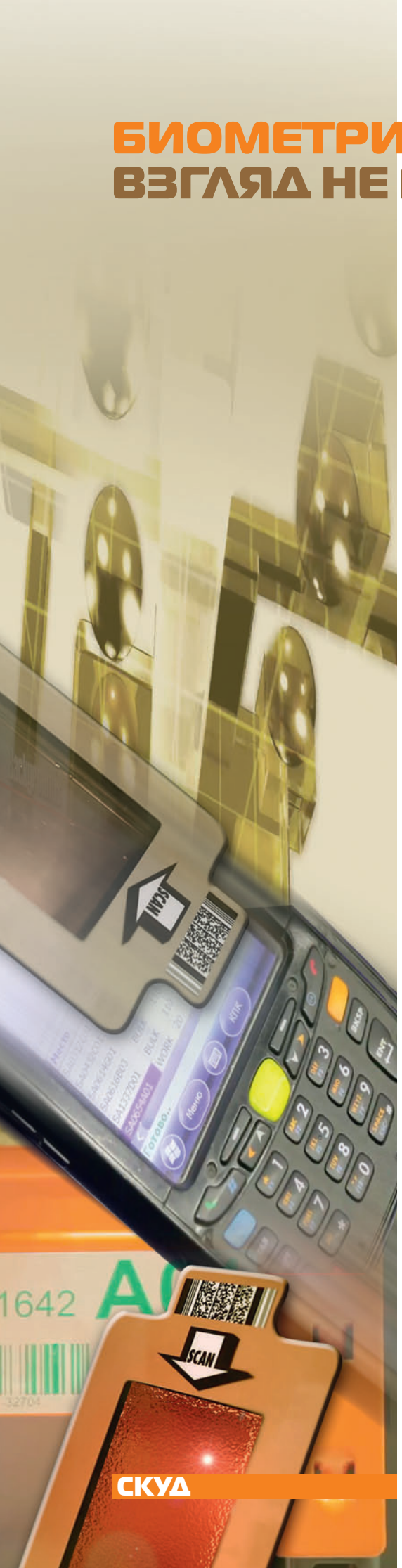
БИОМЕТРИЯ В СКУД. ВЗГЛЯД НЕ ПОСТОРОННЕГО

Тесаков Вячеслав Юрьевич
генеральный директор ООО «Равелин»



Как известно, именно биометрические методы распознавания применяются людьми в повседневной жизни. Так мы узнаем знакомых нам людей – по лицу, голосу, по походке и т. п. Полиция определяет преступников по отпечаткам тоже достаточно давно. Такой способ удобен, надежен, практичен. И уже много лет биометрические технологии применяются в СКУД. Все прекрасно понимают, что это такое, как они работают. Но, что удивительно, до сих пор они так и не вошли в массовую практику. По итогам последних опросов, только 11% инсталляторов используют биометрические технологии более-менее регулярно на своих объектах. В чем причина? Что этому мешает?

Наша компания давно уже выпускает технические средства для систем контроля доступа (СКУД). Попробую выразить свой взгляд на данный казус именно с точки зрения интеграции биометрии с существующими и разрабатываемыми системами.

НАЧНЕМ С САМИХ СРЕДСТВ БИОМЕТРИИ

Ну, во-первых, до сих пор электронные средства биометрической идентификации не добились такого успеха, как природа. Они не могут с точностью до 98-99% идентифицировать человека. Только разработчики технологии 3D-распознавания лиц утверждают, что могут работать в режиме идентификации и не требуют использования карт. Остальные рекомендуют использовать свои средства в режиме верификации (подтверждения) при поднесении карты пользователем. Напрашивается вопрос: «Зачем платить дважды???». Вот инсталляторы и используют средства биометрии только на наиболее ответственных точках доступа проектируемых объектов

Во-вторых, практически все производители биометрических средств предлагают какие-то свои контроллеры и решения. Это абсолютно оправдано с точки зрения коммерции, но что делать с тысячей объектов, где уже спроектированы и установлены системы контроля доступа. Представим, что у заказчика даже есть серьезные основания усилить системы идентификации с помощью биометрии. Но перед ним встает выбор: выкинуть все и поставить «новое замечательное» или оставить все как есть. А он, заказчик, как известно, чаще всего выбирает по цене!!!

Нельзя не отметить, что разработчики биометрических считывателей стараются найти общий язык с производителями средств СКУД. Но возникают барьеры для интеграции. Например, наши китайские друзья просто слабо понимают, что это такое, и постоянно предоставляют SDK с ошибками или не полные. И российские разработчики средств биометрического контроля, как и большинство разработчиков, пишут документацию по мере необходимости. Описание средств интеграции далеко не на первом месте. Вот и получается, что производитель средств сетевых СКУД не только должен очень хотеть, но и изрядно поработать, чтобы произвести интеграцию со средствами биометрической идентификации.

Третья и, безусловно, важная причина – недоверие у самих заказчиков. Согласитесь, опыта еще нет, отсюда психологический барьер. Только несколько лет назад технологии биометрической идентификации стали использоваться в массовом сегменте (смартфоны, банкоматы, паспорта и т. д.). Люди только сейчас начинают осознавать, что средства биометрической идентификации можно использовать в быту. Даже тогда, когда других вариантов идентификации вообще нет, приходится слышать: «А работать то будет?». Мы, как производители средств сетевых СКУД, постоянно на своих семинарах рассказываем о новых возможностях, приводим примеры удачных внедрений. Но к нам приходят инсталляторы, а не конечные пользователи. А пересказ всегда хуже…

Вот и приходится производителям биометрических средств самим пропагандировать свой продукт. Конечно, без поддержки более многочисленной армии инсталляторов возможности их ограничены. И без этой поддержки многие идут по пути готовых решений, и иногда еще больше теряют. Напомним и о нестопроцентной идентификации биометрии: если заказчик про это узнает, то доверие к данным техническим средствам у него снижается.

И последнее, конечно, цена, цена и цена. Для проведения биометрической идентификации требуется обрабатывать значительное количество данных и вести большой объем вычислений, следовательно, контроллер считывателя должен иметь хорошее быстродействие. Стоимость устройства пропорциональна стоимости основного процессора и па-

мяти – вот и получается, что данное решение не может быть дешевым. А еще производители заталкивают в него, на всякий случай, и дополнительные возможности. Вернемся к тому, что заказчики все выбирают по цене. Что остается инсталлятору – предлагать биометрические решения «на всякий случай», и только в редких случаях – из-за невозможности другого решения.

Может сложиться впечатление, что перспектива вырисовывается нерадостная. Но на самом деле сегодня рынок готов применять биометрические технологии идентификации как элемент сетевых СКУД. Знаний, предложений, реализованных проектов – достаточно.

Главная задача производителя средств СКУД для успешной реализации проектов с использованием средств биометрической идентификации – грамотно произвести интеграцию. Поскольку именно он отвечает за работоспособность системы в целом.

КАК ЖЕ НЕ ОШИБИТЬСЯ?

Попробую на нашем опыте показать последовательность выбора партнеров для интеграции – производителей средств биометрической идентификации. Во-первых, надо определиться с тем, что на рынке востребовано. Согласно последним исследованиям основную долю рынка применяемых биометрических считывателей занимают считыватели по отпечатку пальцев. Затем, с большим отрывом, считыватели по рисунку вен и по лицу. В целом, эти три направления закрывают потребности 90% рынка. Можно еще упомянуть идентификацию по радужной оболочке глаз – но сегодня это дорогая экзотика.

Далее, среди средств идентификации по отпечаткам пальцев выбираем наиболее популярные. Понятно, чем дешевле считыватель, тем выше на него спрос. Но при этом должен соблюдаться определенный уровень качества, т. е. оборудование себя уже неплохо зарекомендовало. Самые популярные решения считывателей отпечатков пальцев предлагают производители из России и Китая. Причем последние явно выигрывают по цене и на сегодня занимают около 50% рынка.

Но первый же опыт работы с китайскими производителями показал, что получить от них SDK и объяснения как с ним работать очень сложно. У нас ушел целый год на переписку. Наконец результат получился и… Один из наших партнеров заявляет, что он заменяет прошивку в считывателях своего производства, и они не будут работать со старым SDK. Проходить второй раз путь интеграции с данным производителем не хочется. Поэтому было принято решение в дальнейшем предлагать только то, что работает без подобных усилий.

Второе место по популярности недавно заняли считыватели по рисунку вен. Есть достойный производитель в России, хорошие отзывы, отзывчивое руководство в компании. Но цена изделия 70000 руб. Хотя стоит заметить, зарубежные аналоги как минимум не дешевле. Но во многих случаях это оправдано: качество считывания лучше, меньше ошибок, неприхотливы к испачканным рукам и влажности. Внедрение подобных решений происходит, как правило, под заказ, поэтому мы приняли решение отложить интеграцию до появления конкретного заказа. Стоит признать, что наши конкуренты уже поработали на заказчика из госструктур и довольны. Видимо, у нас все впереди.

Самым удобным способом биометрической идентификации является идентификация по лицу. На сегодня в этом сегменте разработано достаточно большое количество решений. Можно разделить их на две группы: комплексные решения (телевизионная камера, сервер обработки данных) и законченное решение (встроенная телевизионная камера, контроллер, коммутирующее реле).

При комплексном решении достигается наилучшее качество идентификации, поскольку нет ограничений на вычислительные мощности средств обработки данных. Сигнал с датчика (телевизионной камеры) передается на сервер, который производит вычисления и после этого может выдать решение об аутентификации. Алгоритмы и программное обеспечение протестировано на объектах. Основная сложность применения – высокая стоимость конечного решения. И еще – возможна только «программная» интеграция. При этом нарушается один из основных законов работы СКУД, а именно – «контроллер должен работать автономно, в т. ч. в случае пропадания связи с сервером управления». Конечно, для ряда категорий объектов можно обеспечить все необходимые условия, но не для массового рынка. Интеграция с подобной системой возможна при наличии конкретного заказчика и конкретной задачи.

Второй вариант – законченное решение, которое широко представлено на рынке китайскими производителями. Надежность идентификации такого устройства приемлемо. Устройство может применяться в составе сетевых СКУД за счет наличия Wiegand. Однако использование этого устройства имеет некоторые особенности. Во-первых, это создание биометрических шаблонов. Читаем инструкцию. «При вводе изображения в память считывателя людям, имеющим рост 150-180 см, рекомендуется встать в полуметре от устройства, которое монтируется на стене, на высоте примерно 120 см. Во время ввода и проверки шаблона необходимо сохранять спокойное состояние, чтобы обеспечить в дальнейшем корректное распознавание лиц при проходе через точку доступа. Для каждого пользователя в базу заводится несколько изображений лица с различным наклоном головы вверх и вниз при ракурсе съемки анфас. Для более точного позиционирования лица при фиксации кадров необходимо следовать голосовым инструкциям, воспроизводимым устройством, а набор шаблонов, сделанных под разными углами, поможет точнее идентифицировать лицо во время проверки». Особенность в том, что данную процедуру необходимо провести перед каждым устройством. Если таких устройств несколько – это выливается в длительный процесс с привлечением значительного административного ресурса. В исследуемых продуктах централизованное занесение шаблонов невозможно. Напрашивается вывод: данные устройства можно эффективно использовать в автономном режиме либо в случае очень небольшого количества пользователей. Отсутствие SDK на данном этапе тормозит развитие. Но направление очень перспективное.

ПОДВЕДЕМ ИТОГИ

В настоящий момент совершенствование биометрических технологий происходит высокими темпами. И первые результаты – это повышение надежности и снижение стоимости для традиционных технологий: распознавания по отпечатку пальца, лицу и рисунку вен. С другой стороны, постоянно развивается элементная база и повышается скорость обработки данных, что очень стимулирует интеграцию с сетевыми СКУД. Использование биометрических технологий в быту (смартфоны, паспорта и т. д.) повышает их привлекательность и доверие у заказчиков. Все это затронет не только развитие биометрических считывателей. Данные события приведут к технологическим изменениям и совершенствованию имеющихся на рынке систем контроля доступа. Улучшение качества взаимодействия разработчиков сетевых средств СКУД и средств биометрической идентификации неизбежно. Мы должны научиться слушать друг друга, так как выживать и развиваться друг без друга мы не сможем. Как быстро это произойдет, зависит от настойчивости лидеров рынка. Я считаю, что это будут изменения к лучшему, так как в целом они приведут к повышению комфортности и безопасности проживания людей. Изменят их жизнь.