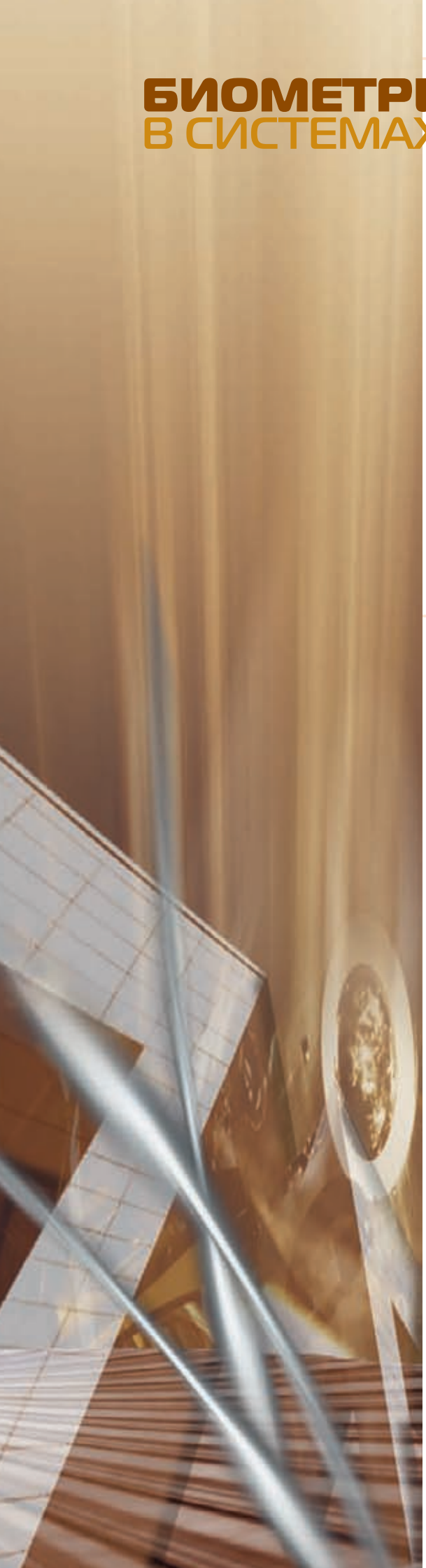

БИОМЕТРИЧЕСКИЕ ТЕХНОЛОГИИ В СИСТЕМАХ КОНТРОЛЯ ДОСТУПА

И. Лукашов
менеджер по маркетингу и PR, ООО «Биолинк Солюшенс»

Биометрическая идентификация признана экспертами самой перспективной технологией контроля доступа. Системы, реализующие данную технологию, – не редкость на российском рынке, и рационально было бы определить основные критерии для выбора оптимального решения.

Принципы работы

Биометрические системы действуют по единому алгоритму: регистрация идентификатора пользователя – преобразование идентификатора в цифровую модель («шаблон») – новое предъявление идентификатора и его трансформация в шаблон – сравнение моделей ранее зарегистрированного и вновь предъявленного идентификатора – вынесение по результатам сравнения решения о предоставлении доступа или отказе в нем.

Качество распознавания зависит от следующих основных факторов:

- типа применяемого биометрического идентификатора (отпечатки пальцев, радужная оболочка глаз, изображение лица и т.д.);
- технологии сканирования идентификатора;
- алгоритма преобразования и сравнения идентификаторов;
- чувствительности биометрической системы к внешнему окружению (помехам, уровню освещенности и т.п.);
- режима распознавания («один ко многим» или «один к одному»).

На сегодня наиболее совершенной является идентификация пользователей по отпечаткам пальцев. Эта биометрическая технология обладает самой длительной историей, проверена многочисленными тестами, применяется в широком спектре разнообразных устройств – от ноутбуков до платежных терминалов и банкоматов.

Почему отпечатки пальцев?

Отпечатки пальцев не меняются в течение всей жизни взрослого человека, их узор быстро восстанавливается в неизменном виде после повреждений; наконец, у каждого из нас, как правило, 10 отпечатков пальцев рук (в сравнении с двумя глазами, одним лицом и т.д.).

Узор кожного покрова и наиболее информативен – в сопоставлении, скажем, с изображением лица. Не менее важен и тот факт, что системы, распознающие пользователей по отпечаткам пальцев, способны действовать и в режиме «один ко многим» (пользователь просто предъявляет идентификатор, после чего его цифровая модель сравнивается с множеством моделей всех зарегистрированных отпечатков пальцев), и в режиме «один к одному» (шаблон вновь предъявленного идентификатора сопоставляется с цифровой моделью, ранее записанной, скажем, в память смарт-карты).

Как правило, только в режиме «один к одному» способны работать биометрические системы, основанные на применении других биометрических идентификаторов. Этот режим обеспечивает несколько большую скорость распознавания, чем идентификация по схеме «один ко многим», но фактически сводит на нет ключевое преимущество биометрии – возможность идентификации по неотчуждаемому признаку, свойственному конкретной личности.

Предпочтительно закупать системы, производимые компаниями, реализующими полный технологический цикл, – от разработки собственных алгоритмов идентификации до их воплощения в аппаратных и программных средствах. Важный признак состоятельности вендора – его участие в независимых тестированиях, регулярно проводимых Национальным институтом стандартов и технологий США (NIST).

Нюансы есть и в работе самих систем идентификации по отпечаткам пальцев. Самая совершенная и эффективная технология – это оптическое сканирование, которое отличается лучшими показателями False Acceptance Rate (FAR – вероятность допуска «чужого»), составляющими 0,0000001-0,0001%.

На рынке представлены емкостные сканеры и терминалы, формирующие изображение отпечатка пальца за счет разности электрических потенциалов на отдельных участках кожи. Данные устройства несколько дешевле, но крайне уязвимы: достаточно простого пробоя (вызванного, скажем, разрядом статического электричества), чтобы элементы сканирующей матрицы вышли из строя и качество распознавания ухудшилось.

Корпоративный масштаб

Главное требование к биометрическим системам контроля и управления доступом (СКУД) – их соответствие организационной структуре предприятия. В это понятие входят следующие аспекты:

- отсутствие ограничений по числу пользователей;
- поддержка территориальной сети – удаленных филиалов компании;
- единое управление всей СКУД (включая

территориальные отделения) из центрального офиса с синхронизацией основного и филиальных серверов СКУД в автоматическом режиме по каналам Интернет;

- минимизация издержек, связанных с рассредоточенностью персонала по территории – например, дистанционная регистрация пользователей СКУД, работающих в удаленных филиалах;
- поддержка управленческой иерархии (отделов, департаментов и т.п.), когда, скажем, начальник отдела в составе управления имеет доступ к данным только по сотрудникам своего подразделения.

Внедрение биометрических СКУД, как правило, не влечет дополнительных требований к корпоративным сетям: объем файла с цифровой моделью отпечатка пальца в продвинутых системах не превышает 500-1500 байт. Размер упомянутого файла важен и для автономной работы биометрических терминалов, когда сравнение моделей идентификаторов осуществляется не на сервере СКУД, а во внутренней памяти самого этого устройства.

Лучшие терминалы способны хранить данные об отпечатках пальцев до 6 тыс. человек; в идеале же должна обеспечиваться возможность и автономного функционирования терминала (например, при сбоях в работе сети), и его работы с сервером СКУД. В последнем случае количество пользователей СКУД не ограничено (что, кстати, выгодно отличает системы, распознающие пользователей по отпечаткам пальцев, от решений, основанных на применении других идентификаторов и способных охватить максимум 2-3 тыс. человек).

Как видно из приведенного примера, даже один терминал вполне способен в одиночку обслужить проходную достаточно крупного предприятия. Скорость распознавания пользователя в таких терминалах не превышает 2 с, и эти затраты сопоставимы с «расходами» времени на другие действия пользователя – поворотом штанги турникета, прохода через него и т.п.

Для ускорения обслуживания сотрудников в часы пиковой нагрузки (скажем, в начале и по окончании смены или рабочего дня) рационально применять смешанный режим взаимодействия терминала и сервера СКУД. В этом случае за подразделениями закрепляются «свои» проходные и соответствующие терминалы, которые хранят во внутренней памяти данные об отпечатках пальцев сотрудников указанных подразделений и обеспечивают максимальную скорость их обслуживания. Если же работник обратится к «чужому» терминалу, тот отправит запрос на сервер СКУД и распознает пользователя (что, правда, потребует несколько большего времени).

Поддержка территориальной структуры

Упомянутая минимизация объемов файлов с моделями отпечатков желательна и при организации соединений между основным сервером СКУД, действующим в центральном офисе компании, и дополнительными серверами, работающими в удаленных филиалах. При использовании низкоскоростных каналов актуальным становится сжатие соответствующего трафика (что должно обеспечиваться средствами управления самой СКУД). В любом случае должна обеспечиваться работа дополнительных серверов в автономном режиме с последующей синхронизацией данных между этими серверами и «центром» по восстановлении оборванного по каким-либо причинам интернет-соединения.

Для централизованного хранения сведений о пользователях, как правило, в комплект поставки биометрических СКУД включается СУБД Microsoft SQL в распространяемой бесплатно редакции – Microsoft SQL Server Express Edition. В данной редакции объем базы данных ограничен 4 GB, и в абсолютном большинстве случаев этого объема достаточно для полноценной работы СКУД, учитывая упомянутые выше размеры файлов с моделями отпечатков пальцев.

В соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и подзаконных актов к нему, на оператора систем обработки этих данных (т.е. администрацию компании) возлагается обязанность обеспечить их безопасность, для чего, в частности, рекомендуется использовать криптографические средства. В рассматриваемом случае оптимальным было бы применение средств «прозрачного» шифрования, реализующих отечественный алгоритм ГОСТ 28147-89; требование обеспечивать безопасность распространяется на все системы, обрабатывающие персональные данные, – независимо от того, применяется ли в них биометрия или нет.

Интеграционные аспекты

Основа биометрической СКУД – терминалы контроля доступа, управляющие исполнительными механизмами (замками, турникетами, шлюзами и т.п.) по предъявлении ранее зарегистрированного идентификатора. Вопросы их интеграции можно рассматривать в трех аспектах.

Во-первых, биометрические технологии должны комбинироваться с другими способами распознавания – по бесконтактным картам и PIN-коду. Карты целесообразно использовать для контроля доступа внешних посетителей, а идентификацию постоянных сотрудников осуществлять по отпечаткам пальцев. Кроме того, терминалы должны предоставлять возможность многофакторной идентификации (скажем, по сочетанию «карта плюс отпечаток пальца»), с помощью которой разграничивается доступ в важные помещения – кабинеты руководителей, серверные и т.п.

Во-вторых, часто биометрические терминалы требуется встраивать в уже существующие на предприятии СКУД, и здесь важна поддержка всех основных интерфейсов – Ethernet, Wiegand, RS-232/485.

В-третьих, терминалы должны быть максимально дружественными по отношению к пользователю и извещать его о результатах идентификации разными способами – выводом информации на дисплей, цветовой индикацией, звуковыми сигналами или голосовыми оповещениями.

Безопасность. Взаимодействие с системой учета рабочего времени

Биометрические СКУД должны блокировать попытки повторного доступа, когда, скажем, опаздывающий сотрудник «проскальзывает» через турникет вместе с коллегой, а затем фиксирует свой уход в положенное время. Идентификация по уникальным биометрическим параметрам как раз и позволяет реализовать принцип «без прихода нет ухода» (функция antipass-back).

Важна возможность формирования графиков доступа, предоставляющих рядовым сотрудникам право посещать офис только в рабочее время, а руководителям, системным администраторам, представителям службы безопасности – круглосуточно.

И, разумеется, СКУД должна эффективно взаимодействовать с системой учета рабочего времени. Ряд продавцов «железа» (карт, считывателей к ним и т.п.) поставляет покупателям простейшие системы учета рабочего времени за символическую плату. Однако и функциональность таких систем крайне ограничена: они используют потенциал учета рабочего времени как мощного средства управления персоналом лишь на 10-15%.

Остальная же часть приходится на следующие важные функции:

- формирование разнообразных графиков учета рабочего времени и отчетов (полноценные системы включают, как правило, не менее 10 различных отчетов);
- проверка присутствия сотрудника на рабочем месте (что подтверждается регулярным предъявлением биометрического идентификатора и актуально для диспетчерских служб, колл-центров и т.п.);
- обмен данными с платформой 1С (желательно, чтобы эта опция подтверждалась сертификатом).

Принимая во внимание тенденцию к постоянному росту зарплат, учет рабочего времени становится не менее востребованным, чем контроль физического доступа. Российские системы, интегрирующие эти важнейшие функции в корпоративном масштабе на единой основе идентификации пользователей по отпечаткам пальцев, служат лучшим доказательством эффективности биометрических технологий, их производительности и надежности.