

БИОМЕТРИЧЕСКИЕ ТЕХНОЛОГИИ НА СЛУЖБЕ БАНКОВ

ВО ВСЕМ МИРЕ ВСЕ БОЛЬШЕ БАНКОВ, В ТОМ ЧИСЛЕ И В РОССИИ, НАЧИНАЮТ АКТИВНО ИСПОЛЬЗОВАТЬ ТЕХНОЛОГИИ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ. СРЕДИ НИХ - SOCIETE GENERALE, РОССИЙСКИЙ СБЕРБАНК, «НАРОДНЫЙ БАНК КАЗАХСТАНА», CALIFORNIA COMMERCE BANK, ING И ДРУГИЕ ГИГАНТЫ. ЧЕМ ЖЕ ПРИВЛЕКАЮТ БАНКИРОВ БИОМЕТРИЧЕСКИЕ СИСТЕМЫ И КАК ОНИ ИХ ИСПОЛЬЗУЮТ?



■ **Константин Сорокин**,
генеральный директор
компании BioLink Solutions

БИОМЕТРИЯ В БАНКОВСКОЙ СФЕРЕ – МИРОВОЙ ОПЫТ

На сегодняшний день биометрия применяется в банках в различных областях, от идентификации клиентов до учета рабочего времени. Например, Западно-Сибирский коммерческий банк использует биометрическую систему аутентификации пользователей BioLink IDenium для защиты доступа в банковские приложения, а российский «ФОРАБАНК» внедрил еще один продукт BioLink – биометрическую систему учета рабочего времени и контроля доступа BioTime.

Если ещё недавно биометрическая идентификация держателей банковских карт казалась фантастикой, то сейчас она стала привычной для десятков и сотен тысяч пользователей в Бразилии и Индии, Польше и Саудовской Аравии, Японии и Колумбии. В России пилотные проекты по ин-

теграции биометрии в банкоматы и POS-терминалы реализует «Сбербанк»: в некоторых регионах держатели эмитированных им «социальных карт» могут оплачивать товары и услуги путем сканирования отпечатков пальцев.

Главная причина использования биометрии – максимальная точность определения личности. Именно личности, а не связанного с ней материального идентификатора (токен, смарт-карта, жетон), который может быть утерян или намеренно передан злоумышленникам. Современные сканеры также имеют функцию установления принадлежности отпечатка пальца живому человеку, и их нельзя обмануть, предъявляя отпечаток отпечатка на бумаге, желатине или стекле.

ИСПОЛЬЗОВАНИЕ ЭЦП

Благодаря высокому уровню точности идентификации биометрические технологии начинают все чаще использоваться с применением электронной подписи. Биометрические системы хранят и сравнивают не сами изображения отпечатков пальцев, а цифровые шаблоны (ID).

Они создаются на основе изображения отпечатка, уникального для каждого человека и не могут быть преобразованы в обратном порядке. ЭП может интегрироваться в такой шаблон биометрической идентификации и обеспечивать защиту «электронного отпечатка» от подделки, идентифицируя владельца и подтверждая отсутствие искажений.

МИНИМИЗАЦИЯ ИНСАЙДЕРСКИХ УГРОЗ

Проблема минимизации инсайдерских рисков традиционно актуальна для руководителя службы информационной безопасности любого банка. Несанкционированный доступ к конфиденциальной информации и корпоративным ресурсам – счетам и персональным данным клиентов, финансовым отчетам, приложениям для проведения транзакций – может привести к колоссальному ущербу, как финансовому, так и деловой репутации.

Одним из самых эффективных решений данной проблемы может быть внедрение системы биометрической идентификации сотрудников. Таким образом, департамент безопасности может быть уверен, что доступ к информационному ресурсу имеет наделённый таким правом сотрудник, а не злоумышленник, завладевший его паролем или смарт-картой.

На сегодняшний день самым масштабным биометрическим проектом в СНГ – 9000 рабочих станций – является внедрение системы BioLink IDenium в АО «Народный банк Казахстана». Система биометрической идентификации действует централизованно и охватывает не только головной офис, но и все территориально удаленные филиалы банка. Установленная в банке система интегрирует процесс биометрической идентификации в инфраструктуру Microsoft Active Directory и терминальные приложения (Citrix, Microsoft RDS и т.д.), поддерживает Windows 7 и Windows 2008 Server R2, а также обеспечивает единый «биометрический вход» (Single-Sign-On) во все корпоративные приложения.

КОММЕНТАРИИ БАНКОВ

■ С.В. ПАЗИЗИН,

руководитель группы защиты автоматизированных банковских систем банка ВТБ, кандидат физико-математических наук:

— Принципиальным преимуществом аутентификации пользователей по биометрическим характеристикам (отпечаткам пальцев, геометрии руки, лицу, голосу, рисунку сетчатки глаза и т.п.) является неотделимость этих характеристик от пользователя. Их нельзя забыть, потерять или передать другому пользователю.

Определение личности по биометрическим характеристикам осуществлялось задолго до появления автоматизированных компьютерных систем. Например, собственноручная подпись для документа на бумажном носителе позволяет подтвердить его подлинность именно на основе биометрических характеристик подписавшего, а отпечатки пальцев в криминалистике используются уже более ста лет.

До недавнего времени широкому распространению аутентификации по биометрическим характеристикам в автоматизированных банковских системах препятствовала нерешенность следующих проблем:

1. Биометрические характеристики сложно точно измерить, т.к. в них всегда присутствует определенная случайная составляющая. Например, связанная с силой прижатия и скоростью движения пальца по считывателю.

2. Биометрические характеристики могут изменяться со временем, что заставляет регулярно корректировать эталонный образ аутентифицирующей информации.

3. Возможен отказ в доступе, связанный с кратковременным изменением биометрических характеристик. Например, из-за волнения может измениться почерк, из-за простуды — голос, а человека, сломавшего палец, трудно идентифицировать по отпечатку этого пальца.

Учитывая, что 10–15 лет назад в период активного внедрения средств аутентификации использование биометрии требовало еще и значительных дополнительных затрат, большинство банков приняли решение в пользу двухфакторной аутентификации на основе паролей и внешних носителей информации.

За прошедший период времени соотношение цена/качество для аппаратных устройств считывания биометрических характеристик значительно улучшилось, а современная элементная база обеспечила возможность реализации сложных алгоритмов для обработки считываемых данных, что позволило значительно снизить вероятности ошибочного признания и ошибочного отказа в доступе.

Таким образом, в настоящее время биометрические технологии имеют все шансы совершить прорыв в банковскую сферу на новом витке научно-технического прогресса. Распространению биометрической аутентификации также будет способствовать тенденция к переходу на единую аутентификацию пользователей для всех приложений (Single Sign On).

■ А.М. СЫЧЕВ,

заместитель директора департамента безопасности, начальник Управления информационной безопасности ОАО «Россельхозбанк», кандидат технических наук:

— Усложнение информационных технологий и повышение требований к обеспечению информационной безопасности ставят на повестку дня важный вопрос о совершенствовании традиционных технологий обеспечения информационной безопасности.

Сложно назвать системы биометрической защиты новыми. Однако следует признать, что за последнее время эти технологии шагнули далеко вперед, что делает их перспективным направлением не только в обеспечении информационной безопасности, но и важным фактором успешной работы служб безопасности банков, направленной на защиту экономических интересов банка.

Имеющиеся в настоящий момент на рынке решения могут быть использованы как дополнительный фактор идентификации и аутентификации, что особенно важно для системно-значимых систем и сервисов.

Отдельное перспективное направление — это использование биометрических технологий в системах, обеспечивающих защиту от внутреннего и внешнего фрода. Всем известны варианты мошенничества, когда один и тот же человек по разным поддельным или украденным паспортам в разных филиалах (или дополнительных офисах) оформляет кредитную заявку. В этом случае верификация клиента по его фотографии значительно надежнее выявит подозрительные действия и даст возможность предотвратить совершение преступления.

■ В.А. ОКУЛЕССКИЙ,

начальник Отдела защиты информации службы безопасности ОАО «Банк Москвы», кандидат технических наук:

— Основное «вкусное» свойство биометрии — идентификация непосредственно личности, а не ее атрибутов или носителей атрибутов. Основная проблема — вывод биометрии из математические модели. На мой взгляд, BioLink успешно одновременно решает проблему и практически применяет полезные свойства биометрии.

«Банк Москвы» давно уже присматривается к использованию отпечатка пальца как дополнительному средству аутентификации клиентов и пользователей. Так, в нашем самом передовом офисе на Тверской, д. 8 биометрия используется для доступа клиентов к своим ячейкам в автоматизированном депозитарии. Проведен успешный пилотный проект по встраиванию биометрического подтверждения проведения операций в АБС. Одним словом — за биометрической идентификацией большое будущее, в том числе в области банковских технологий.

На территории России наиболее масштабным использованием биометрической идентификации отметился ОАО «Забсбкомбанк». В этом банке также установлена система BioLink IDenium, в головном офисе и 24 филиалах. По отзывам службы ин-

формационной безопасности банка, внедрение этой системы обеспечило двойной эффект: усиление уровня информационной безопасности и минимизация рисков несанкционированного доступа, с одной стороны, значительное снижение нагрузки на

службу Help Desk и затрат на решение инцидентов с паролями — с другой. Оценивая показатель ROI от внедрения системы IDenium как высокий, руководство банка приняло решение о масштабировании системы на все филиалы.