



Дмитрий Швецов

Биометрические технологии – драйвер развития цифровой экономики

В статье рассматриваются современные цифровые методы, применяемые в банковской сфере, которые должны обеспечивать самые высокие требования к безопасности обработки и хранения персональных данных клиентов. На рынке банковских услуг самым основным фактором и конкурентным преимуществом является доверие клиентов к банку. Дальнейшее совершенствование систем информационной безопасности и внедрение современных способов защиты персональных данных клиентов позволят коммерческим банкам занимать лидирующие позиции на цифровом рынке банковских услуг.

ОБЗОР РЫНКА БИОМЕТРИЧЕСКИХ ТЕХНОЛОГИЙ

К одним из самых успешных инновационных инструментов защиты персональных данных клиентов относят биометрические технологии. В основе востребованных банковским сектором биометрических технологий лежит механизм распознавания уникальных биологических характеристик, присущих каждому человеку. В зависимости от состава индивидуальных характеристик человека выделяют два типа биометрических данных. Статические биометрические данные присущи человеку с рождения, это могут быть ДНК, отпечаток пальца, рисунок вен ладоней, сетчатка глаза. Динамические данные – это те, которые человек приобретает и способен с возрастом изменить, в их числе динамика речи,

рукописная подпись, темп набора текста на клавиатуре и многие другие. Темпы роста мирового рынка биометрических технологий с каждым годом только увеличиваются. Согласно прогнозам объём мирового рынка биометрии к 2022 году превысит 40 млрд долларов США. Прогноз международной консалтинговой компании “J’son & Partners Consulting” (J&PC) представлен на рис. 1.

Сегментация мирового рынка биометрии распределяется следующим образом: основными потребителями биометрических технологий станут государственный сегмент и национальные системы безопасности. Государственный сегмент включает в себя электронные документы, такие как паспорта граждан, водительские удостоверения и прочие персональные документы, удостоверяющие

личность пользователей. Национальные системы безопасности заинтересованы в развитии систем идентификации граждан, туристов и мигрантов, клиентов финансового, корпоративного сегмента, здравоохранения и ритейла. Как прогнозирует J&PC, ожидается активное развитие коммерческого применения систем идентификации: на мировом рынке биометрии объём государственных проектов будет снижаться, а финансовый сектор, наоборот, к 2022 году увеличит свою долю на рынке до 27,5%. Этот тренд представлен на рис. 2. Следует отметить, что на российском рынке ожидается аналогичная ситуация.

Если проанализировать текущее состояние мирового рынка биометрических технологий, то наиболее часто используются системы, основанные на

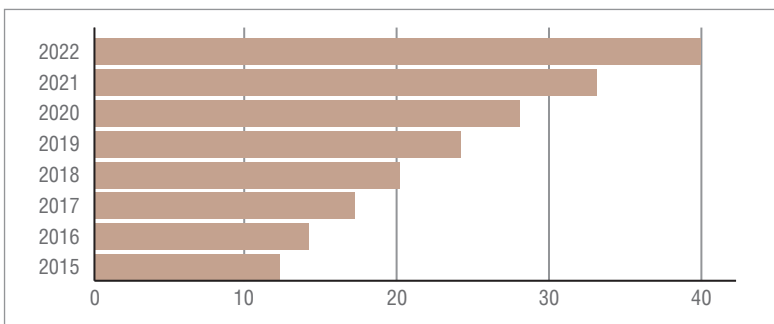


Рис. 1. Объём мирового рынка биометрических технологий в 2015–2022 годах, млрд \$

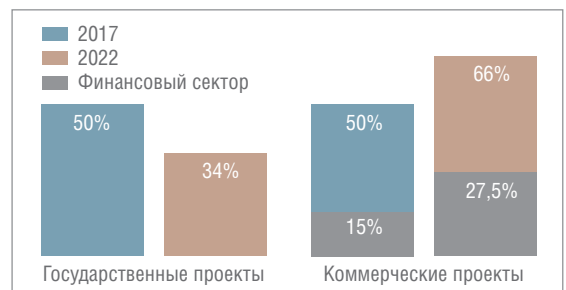


Рис. 2. Структура мирового рынка биометрических технологий в 2017–2022 годах, %

контроле отпечатков пальцев рук (40%), а также рисунка вен ладони (19%), что в совокупности составляет более 50% всего рынка (рис. 3). Тем не менее, по оценкам экспертов, в ближайшие пять лет способы идентификации по отпечаткам пальцев и сканированию ладони будут расти меньшими темпами по сравнению с набирающими обороты технологиями идентификации по лицу и голосу, среднегодовые темпы роста которых прогнозируются на уровне 22% к 2022 году. Для сравнения, темп роста технологии идентификации по отпечаткам пальцев и рисунку вен ладони в среднем ожидается на уровне 16% в год.

Тренды развития и применения биометрических технологий

На финансовом рынке применения биометрии наблюдается активное развитие мобильных технологий и, соответственно, популяризация мобильного банкинга, занимающего уже несколько лет лидирующие позиции цифровизации банковского сектора. Современные мобильные телефоны умеют записывать голос, фотографировать изображение, а высококачественные камеры и вовсе позволяют идентифицировать человека по радужной оболочке глаза. Таким образом, современные телефоны постепенно становятся мультибиометрическими устройствами. Кроме мобильных телефонов, биометрические технологии начинают применяться и в других устройствах, таких как банкоматы и терминалы самообслуживания, с помощью встроенных сенсоров и видеокamеры, в магазинах посредством распространения биометрических терминалов, без использования банковской карты, а также в устройствах, идентифицирующих человека по голосу при звонке в call-центр.

Одним из ключевых трендов развития банковских услуг является оснащение платёжных систем биометрическими технологиями. Первыми примерами внедрения платёжных систем на мировом рынке стали Apple Pay, Samsung Pay, Android Pay, что означает большой прорыв в области развития биометрических технологий во всем мире, так как данные платёжные сервисы удобны для многих пользователей смартфонов. Биометрические технологии в области идентификации личности давно стали привычными в системах контроля и управления доступом (СКУД). А что касается банковской сферы, то область их применения расширяется практически



Рис. 3. Структура биометрических технологий в финансовом секторе, %

ежедневно и не ограничивается системами входа/выхода. Достаточно новый метод идентификации по уникальному рисунку вен ладоней быстро приобретает популярность во всем мире. Например, в 2004 году крупнейшие банки Японии, такие как Ogaki Kyoritsu Bank, Suruga Bank, The Hiroshima Bank и The Bank of IKEDA, внедрили систему биометрической идентификации по венам ладони для подтверждения операций по банковской карте в банкоматах. Нововведение позволило значительно повысить уровень безопасности и комфорта при организации доступа к личному счёту даже при отсутствии банковской карты. Повышенный интерес к технологии был обусловлен необходимостью разработки надёжной системы доступа даже во время стихийных бедствий и катастроф. И это подтвердилось во время крупного землетрясения в Японии в 2011 году, когда многие жители не смогли воспользоваться банкоматами для снятия наличных средств, поскольку карты и другие подтверждающие документы были безвозвратно утеряны.

Российские коммерческие банки также начинают применять в своей деятельности биометрические технологии. Отметим, что крупные банки уже используют идентификацию клиентов по изображениям лица и по голосу при их обращении в call-центр, а также идентификацию по отпечатку пальца при входе в мобильное приложение банка на смартфоне. Также во многих банках проводятся пилотные проекты по запуску новых технологий. Нейросетевые технологии позволяют максимально точно идентифицировать человека по его биометрическим данным. Кроме того, биометрические технологии сегодня применяются в банках не только для защиты

персональных данных клиентов, но и для обеспечения безопасности корпоративной информации. Так, ПАО «Почта Банк» запустило в 2017 году для сотрудников банка биометрическую идентификацию по изображению лица для входа в операционные банковские системы. Таким образом, российские банки заинтересованы во внедрении инновационных биометрических технологий в целях предотвращения мошенничества и повышения уровня лояльности клиента к банку за счёт предоставления удобных и безопасных услуг. Ключевым драйвером в развитии биометрических технологий во всех банках России является запуск удалённой идентификации клиентов. Согласно Федеральному закону от 31.12.2017 № 482-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации», банки имеют право удалённо идентифицировать клиентов — физических лиц для предоставления банковских услуг и продуктов дистанционно посредством Единой биометрической системы (ЕБС) и Единой системы идентификации и аутентификации (ЕСИА). Отметим, что до внесения правок в законодательство для получения банковских услуг дистанционно клиентам было необходимо хотя бы один раз лично прийти в офис банка, услугами которого он хочет пользоваться дистанционно, и пройти процедуру идентификации. Теперь с помощью платформы удалённой идентификации, которая представляет собой трёхфакторную аутентификацию: авторизация в ЕСИА и два биометрических фактора (голос и изображение лица), клиент сможет пользоваться услугами любых банков дистанционно. Но всё-таки один раз придётся сходить в офис банка-участника ЕБС, чтобы оставить свои индивидуальные биометрические данные. Нельзя не отметить, что запуск ЕБС в России произошёл в достаточно короткие сроки. Так, после принятия закона № 482-ФЗ банки в течение первого полугодия 2018 года тестировали новую систему, вносили свои предложения по совершенствованию механизма удалённой идентификации, а также дорабатывали свою технологическую инфраструктуру для реализации данного механизма. Более 20 крупных отечественных банков приняли участие в тестировании ЕБС. А 30 июня 2018 года ЕБС уже официально заработала, банки активно начали использовать новый механизм в своей деятельности, и на август 2018 года количество банков, на которых возложены

полномочия сбора и передачи биометрических данных в ЕБС, достигло более 430 кредитных организаций. Оператором ЕБС назначено ПАО «Ростелеком», которое отвечает за организацию и передачу сбора биометрии, а также за контроль соответствия этих данных первичным образцам. Единая биометрическая система — это цифровая платформа для удалённой идентификации граждан, позволяющая им пользоваться государственными и коммерческими услугами 24 часа в сутки из любого уголка мира. В основу построения ЕБС был заложен принцип мультимодальности. В настоящее время в ЕБС используется два вида биометрии: лицо и голос. Использование двух модальностей одновременно позволяет идентифицировать живого человека, а не подделку его биометрических данных. ЕБС — открытая платформа, участниками которой являются ведущие отечественные разработчики биометрических технологий, причем для технической поддержки каждой из двух модальностей привлечены несколько независимых вендоров для повышения качества функционирования системы. Комбинирование голоса и лица, позволяющее определить имитацию вместо живого человека, является ключевой способностью ЕБС. В результате сочетания этих двух характеристик ЕБС способна выявлять мошенников и оперативно реагировать на них. Полезным качеством ЕБС является выявление аномалий: система способна не только распознавать мошенничество, но и усилить банковские системы защиты от фрода (fraud — мошенничество, обман, жульничество) с помощью технологии машинного обучения. Так как каждый человек имеет определённый профиль в системе, сложившийся по проводимым ранее операциям, ЕБС способна реагировать на любое отклонение от стандартных действий конкретного человека в целях выявления аномального поведения. Хранение биометрических данных в ЕБС происходит в обезличенной форме отдельно от персональных данных, хранящихся в базе ЕСИА. Связка между системами осуществляется по уникальному, зашифрованному криптографическими средствами защиты коду.

Единая биометрическая система является ключом к цифровой экономике для государства, граждан и бизнеса. Основное преимущество для государства от внедрения ЕБС — это распространение цифровых государственных и муниципальных услуг, направленных на повы-

шение уровня цифровизации системы государственного управления. Для граждан ЕБС обеспечит предоставление банковских услуг в любое время и в любом месте, что повлияет на повышение уровня финансовой доступности, в том числе для удалённых и малонаселённых регионов России и маломобильных граждан. Кроме того, ЕБС повысит конкуренцию на рынке за клиента, так как граждане теперь могут рассматривать предложения любых банков и пользоваться их услугами без личного посещения, заключая договор с кредитной организацией дистанционно. Использование современных биометрических технологий даёт людям цифровую свободу, которая заключается в получении финансовых услуг «на ладони» — посредством мобильного телефона. Для бизнеса, в частности для коммерческих банков, преимущества от использования ЕБС заключаются, во-первых, в привлечении новых клиентов, так как удалённая идентификация позволяет привлечь клиента через Интернет независимо от географии присутствия банка, что поможет банку увеличить свою нишу на рынке. Во-вторых, это создание новых цифровых услуг, отвечающих потребностям современного общества: оформление договоров, открытие вкладов и счетов, выдача кредитов и в целом обслуживание клиента 24 часа 7 дней в неделю. Также одним из основных преимуществ ЕБС для банков является сокращение операционных издержек на обслуживание отделений, вследствие чего появляется возможность перераспределить ресурсы на повышение качества услуг, а не на развитие сети продаж. Безусловно, создание инфраструктуры для применения биометрических технологий требует первоначально немалых затрат со стороны банка. Но те банки, которые доработали свои системы и запустили применение биометрии, несомненно, являются лидерами в новой цифровой экономике, поэтому, чтобы быть конкурентоспособными, сегодня все банки стремятся развивать цифровой бизнес. Отметим, что на протяжении уже нескольких лет мировым трендом является сокращение посещений клиентами офисов банков и их переход в цифровую среду. В 2017 году уже 46% клиентов не посещают банковские отделения, а в 2012 году только 27% населения выбирало дистанционные банковские каналы. Кроме того, стоимость привлечения новых клиентов традиционными способами с каждым годом растёт. По итогам 2017 года в 80% банков стоимость при-

влечения клиента увеличилась. Таким образом, нельзя не согласиться с мнением первого зампреда Банка России Ольги Скоробогатовой, что «коммерческие банки могут потерять до 20–60% прибыли к 2025 году, если не сумеют встать на один уровень с ведущими цифровыми компаниями, внедрив цифровые платформы и цифровые услуги».

ЗАЩИТА И БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ

Нельзя не отметить и проблему обеспечения безопасности данных. Одним из способов защиты информации является подтверждение личности клиента банка по его биометрическим данным. Рассмотрим пример использования метода идентификации клиентов банка с помощью рисунка вен ладони. При открытии банковского счета клиент подписывает соглашение пользователя системы биометрической идентификации. После этого осуществляется регистрация ладоней клиента, а при необходимости ладоней доверенных лиц. Полученные при сканировании уникальные цифровые шаблоны ладоней вносятся в электронную базу банка или ЕБС. Биометрические данные сканируются при помощи настольного USB-сканера, находящегося у клиента. Цифровые шаблоны не могут быть преобразованы в исходные изображения рисунков вен ладоней и, как следствие, не могут быть использованы вне информационной системы. Биометрическая идентификация клиента банка может использоваться при совершении финансовых операций, таких как снятие денежных средств, переводы, доступ к конфиденциальной информации о счёте. Это решение даёт хорошие гарантии безопасности: исключается несанкционированный доступ к счёту клиента, появляется возможность обслуживания клиентов центрального офиса в любом из расчетно-кассовых отделов банка и наоборот, без предварительного запроса доверенности, существует надёжное подтверждение личности при доступе к системе клиент-банк и при совершении прочих финансовых операций.

И ещё одно решение — самое важное для банков. В повседневной деятельности кредитной организации возникают задачи ограничения доступа к информационным ресурсам и конфиденциальной информации. Традиционные пароли и электронные ключи не обеспечивают требуемого уровня безопасности, так как существует угроза передачи ключа и пароля и осуществления несанкционированного

доступа (НСД). Согласно РД ФСТЭК РФ от 30.03.1992 субъектом доступа является лицо (или процесс), действия которого регламентируются правилами разграничения доступа. Исходя из предположения о том, что идентификатор субъекта доступа, являющийся его секретом (пароль, электронный ключ, карточка), может быть скомпрометирован с целью дальнейшего использования в целях НСД, необходимо дополнительно усиливать комплекс защитных мер (КЗМ). Единственным уникальным идентификатором, позволяющим гарантированно установить соответствие субъекта доступа лицу, имеющему право доступа, выступает биометрическая характеристика, присущая только этому лицу. Таким образом, для выполнения в полном объёме законодательных требований в части создания КЗМ необходимо применение усиления КЗМ средствами распознавания биометрических характеристик (биометрических идентификаторов). Например, наряду с распознаванием лица и звуковой дорожки наиболее безопасным методом, с точки зрения эффективности пресечения попыток компрометации, является метод распознавания рисунка вен ладоней. Применение усиления КЗМ позволяет избежать ситуации с возможной компрометацией идентификаторов субъекта доступа. Принцип работы системы доступа к информационным ресурсам выглядит следующим образом. Для входа в систему пользователю необходимо приложить ладонь к USB-сканеру вен ладоней. Биометрические данные считываются и обрабатываются специально уста-

новленной программой на ПК. В случае успешной идентификации осуществляется запуск операционной системы. Зачастую программное обеспечение интегрируется с системой Active Directory, что позволяет использовать различные сценарии доступа. Также возможен совместный режим доступа с использованием USB-токенов или смарт-карт, где биометрические шаблоны хранятся непосредственно в памяти токена или карты, тогда нет необходимости привязываться к определённому компьютеру. Вначале пользователю необходимо приложить карту или USB-токен, затем ладонь. Биометрические данные считываются из памяти электронного носителя и сравниваются с полученным шаблоном ладони. Данный режим позволяет значительно повысить уровень безопасности, а ёмкость системы по количеству пользователей становится неограниченной. И это решение также имеет ряд преимуществ по сравнению с традиционными СКД: исключение возможности несанкционированного доступа к информационным ресурсам; нет необходимости запоминать пароль; снижение затрат на администрирование и сопровождение системы в связи с восстановлением паролей; быстрый и удобный доступ к информационным ресурсам; режимы работы: ладонь, логин + ладонь, смарт-карта + ладонь, USB-токен + ладонь. Стоит сказать, что технологии идентификации постоянно совершенствуются, возможно, в скором будущем мы увидим и другие методы, используемые в биометрии. Но на сегодняшний день метод идентификации по уникаль-

ному рисунку вен ладоней признан самым надёжным и удобным для использования в банковском секторе.

ЗАКЛЮЧЕНИЕ

Подводя итог, можно отметить, что механизм удалённой идентификации в банках — это только начало цифровизации финансового сектора России. Далее данный механизм может распространяться на страхование, микрокредитование и другие сферы финансового рынка. Кроме того, рассматриваются перспективы применения единой биометрической системы и в других отраслях экономики: государственные и муниципальные услуги, образование, ритейл, телемедицина, электронная коммерция.

Внедрение удалённой платформы идентификации является одним из ключевых факторов перехода к цифровой экономике и, главное, к повышению уровня финансовой доступности. Все перечисленные биометрические технологии являются инновационными методами минимизации мошенничества и повышения доверия клиентов. Эффективное регулирование нового механизма удалённой идентификации и активное стимулирование развития единой биометрической системы позволит российской экономике завершить цифровизацию общества и выйти на новый уровень развития. ●

**Автор – сотрудник
фирмы ПРОСОФТ
Телефон: (495) 234-0636
E-mail: info@prosoft.ru**


www.axiomtek.com

Простой шаг в будущее умного мира



-30...+60°C

eBOX800-900-FL

Система с полной защитой IP67 для граничных вычислений и искусственного интеллекта, для установки вне помещения

Прочная безвентиляторная система для граничных вычислений с полной защитой IP67, с NVIDIA® JETSON™ TX2, запираемыми разъёмами M12 и входом электропитания 100–240 В AC



-40...+70°C

tBOX300-510-FL

Безвентиляторная транспортная система с ЦП Intel® Core™ и Celeron® для применения в автомобильных, железнодорожных и морских ПК



-40...+70°C

ICO500-518

Безвентиляторная встраиваемая система для монтажа на DIN-рейку с ЦП Intel® Core™ и дублированной модульной конструкцией для расширения возможностей ввода/вывода


Axiomtek Co., Ltd. E-mail: info@axiomtek.com.tw Tel: +886-2-8646-2111
Реклама