БАНКИ ЗОВУТ НА СБОРЫ

ЛЕТОМ ЭТОГО ГОДА В РОССИИ БЫЛА ЗАПУЩЕНА ЕДИНАЯ БИОМЕТРИЧЕСКАЯ СИСТЕМА, КОТОРАЯ ДОЛЖНА УПРОСТИТЬ ДОСТУП К ФИНАНСОВЫМ УСЛУГАМ МАЛОМОБИЛЬНЫМ И ПРОЖИВАЮЩИМ В ОТДАЛЕННЫХ РАЙОНАХ ГРАЖДАНАМ. ЭКСПЕРТЫ ПРОГНОЗИРУЮТ ЗНАЧИТЕЛЬНЫЙ РОСТ СПРОСА НА БАНКОВСКУЮ БИОМЕТРИЮ В ТЕЧЕНИЕ ДВУХ-ТРЕХ ЛЕТ, НАЗЫВАЯ ЕЕ САМЫМ НАДЕЖНЫМ СПОСОБОМ ИДЕНТИФИКАЦИИ КЛИЕНТОВ. ИГОРЬ ШИШКИН

ГЛЕБ ЩЕЛКУНОВ

ПОДКЛЮЧЕНИЕ К ЕДИНОЙ БИОМЕТРИЧЕСКОЙ СИСТЕМЕ ОБХОДИТСЯ СРЕДНЕСТАТИСТИЧЕСКОМУ БАНКУ В 3–4 МЛН РУБЛЕЙ

С 1 июля компания «Ростелеком» запустила единую систему, в рамках которой стартовал сбор биометрических данных клиентов с помощью записи голоса, а также видео с изображением лиц. «Технически регистрация тех, кто пожелал сдать биометрию, проходит в два этапа: сначала клиентами создаются учетные записи в Единой системе идентификации и аутентификации (ЕСИА) или на портале госуслуг. После этого необходимо посетить одно из банковских отделений, чтобы сдать биометрическую информацию. Базой собранных данных смогут воспользоваться все российские кредитно-финансовые организации»,— комментирует вице-президент QBF Владимир Масленников.

По его словам, главное преимущество инновации для клиентов состоит в том, что после сдачи биометрических данных для них существенно увеличивается количество услуг, которые можно получить дистанционно. «Это актуально прежде всего для жителей регионов, где нет представительств многих российских банков и финансовых компаний, например Крыма. Также нововведение способно упростить обслуживание маломобильных граждан. Вероятно, шансом минимизировать личное общение с сотрудниками финансовых организаций воспользуются молодые люди, хорошо ориентирующиеся в онлайн-сервисах. Значительный рост спроса на новую услугу прогнозируется в перспективе двух-трех лет»,— отмечает господин Масленников.

«На мой взгляд, основные причины внедрения биометрии банками — это сокращение операционных затрат на обслуживание офисов, повышение качества услуг и увеличение количества обслуживаемых клиентов. На сегодняшний день законодательство и технологии удаленной идентификации с использованием биометрических данных человека позволяют открыть счет или получить кредит, не обращаясь в офис банка. Это дает возможность кредитным организациям, с одной стороны, снизить количество посетителей в офисах, с другой стороны — увеличить число обслуживаемых клиентов за счет повышения удобства и скорости предоставления услуг»,— считает руководитель направления управления доступом центра информационной безопасности «Инфосистемы Джет» Ярослав Жиронкин.

Технологии биометрии помогают повышать удобство и сокращать скорость обслуживания клиентов до 20–40 секунд, конкретизирует менеджер по продвижению решений для контактных центров КРОК Дмитрий Песоцкий. «Ранее, чтобы верифицировать клиента, оператору центра обработки вызовов банка приходилось уточнять, например, данные паспорта, кодовые слова и прочее. Сейчас в этом нет необходимости. Помимо этого, голосовая биометрия позволяет повысить эффективность работы контактного центра и сократить штат операторов на 10–20%»,— перечисляет он.

С другой стороны, сбор биометрического материала для финансовых организаций сопряжен с определенными расходами. «В среднем на подключение кредитно-финансовой организации к системе единой службы необходимо 3–4 млн рублей для организаций небольшого и среднего размера (в случае особо крупных структур, таких как, например, Сбербанк или ВТБ, сумма может значительно возрастать), из которых почти половина уйдет на инструменты по защите от киберугроз, остальное — на оборудование. Стоимость подключения дополнительных отделений в среднем составит 150–200 тыс. рублей»,— говорит Владимир Масленников.

НАЛОЖИТЬ ОТПЕЧАТОК Технический директор Trend Micro в России и СНГ Михаил Кондрашин отмечает, что миллионы клиентов в Bank of America, JPMorgan Chase и Wells Fargo регулярно используют отпечатки пальцев для входа в свои аккаунты через мобильные приложения. Последняя компания даже позволяет корпоративным клиентам сканировать сетчатку глаза с помощью мобильного телефона.

«Наибольшей популярностью пользуется идентификация клиентов по голосу. Вместо того чтобы тратить до семи минут, отвечая специалисту контакт-центра на секретные вопросы, клиенты тратят всего 20 секунд, подтверждая свою личность голосом. Например, в Barclays более 65% звонков клиентов обрабатывается при помощи голосовой верификации. Используя тот же метод, Banco Santander Mexico не просто сократил время аутентификации на 42 секунды, но и еще сэкономил $1 млн. Citigroup идентифицирует по голосу 800 тыс. своих клиентов с кредитками, а 90% клиентов словацкого Tatra Bank рассказали, что предпочли голосовую биометрию традиционной системе верификации пользователей»,— перечисляет господин Кондрашин. «В HSBC, где почти половина всех новых учетных записей открывается онлайн, бизнес-клиенты теперь могут открыть новый аккаунт, сделав селфи для проверки своей личности. USAA, которая предоставляет страхование и банковские услуги военнослужащим и их семьям, определяет некоторых клиентов по контуру лица»,— продолжает он. В целом, согласно исследованию Biometrics for Banking, к концу 2020 года 1,9 млрд пользователей по всему миру будут использовать биометрию для получения банковских услуг.

ПЛАТА ЗА БЕЗОПАСНОСТЬ Как и любая персональная информация, биометрические данные могут храниться на какомнибудь диске или облаке, а значит, есть серьезный риск их утечки и последующей компрометации, указывает Михаил Кондрашин. «Например, в 2015 году Департамент по управлению персоналом в США, который является отделом кадров для правительства, столкнулся с утечкой 5,6 млн данных отпечатков пальцев. Через год на Филиппинах произошел еще один подобный инцидент. Группа хакеров взломала базу данных местной комиссии по выборам. Утекли персональные данные 55 млн зарегистрированных избирателей, в некоторых случаях были раскрыты паспортные данные и маркеры отпечатков пальцев. В прошлом году хакеры смогли обойти функцию блокировки Samsung Galaxy S8 с помощью радужной оболочки глаза»,— рассказал он. По словам эксперта, основные способы защиты от взлома или утечки — шифрование биометрических данных, использование мультифакторной аутентификации пользователя.

Если соотнести вред от частных случаев утечек информации с пользой для всего общества, очевидно, что на общем уровне безопасности сбор биометрии скажется положительно, считает ведущий аналитик компании «Серч Информ» Алексей Парфентьев.

«Применение биометрии для идентификации и есть один из основных трендов информационной безопасности, повышающих защищенность систем, ведь утечка или кража авторизационной биометрии (например, хеша отпечатка пальцев) ничего злоумышленнику не даст. В этом и суть технологии. Другое дело, что совместно с этой информацией всегда идут и другие персональные данные: учетная запись, контактная информация, имя, фамилия. Банки должны стремиться к тому, чтобы не происходило даже частных утечек, особенно когда речь идет о такой критичной информации, как образцы голоса и изображение человека»,— говорит господин Парфентьев.

Эксперты солидарны, что банковская биометрия должна быть добровольной для клиентов. «На мой взгляд, банки не должны навязывать удаленную идентификацию без разъяснения возможных негативных последствий. Очень важно, чтобы у клиентов была возможность выбора альтернативных вариантов идентификации, включая личное присутствие. Чтобы обезопасить себя, человек должен сам принимать решение о необходимости подобной услуги в балансе между удобством и финансовыми рисками, которые он может понести в случае компрометации его личности»,— считает господин Жиронкин.

«Для банков поддержка такого способа авторизации должна быть принудительной, им нужно быть на передовой технологий, в том числе кибербезопасности. Для пользователей авторизация с помощью биометрии должна быть опциональной. Как минимум потому, что нельзя обязать всех людей обзаводиться устройствами, поддерживающими возможность передавать биометрические данные»,— согласен господин Парфентьев. ■