

нимая кошелек, банковскую карту или иное устройство, гражданам нужно будет сдать свои биометрические данные в Единую биометрическую систему, пояснили «Деньгам» в «Русском стандарте». Затем для проведения финансовых операций потребуется привязать платежную карту к своему цифровому образу в ЕБС. Привязать карту к ЕБС можно в мобильном приложении «Биометрия» от «Ростелекома» или в приложении банка, которое поддерживает функцию «оплата по лицу». Платеж при этом можно будет производить и через систему Банка России, и через Систему быстрых платежей (СБП).

И банки, и «Ростелеком» возлагают на такую систему расчетов большие надежды. Кроме удобства подобных расчетов, указывают в «Русском стандарте», тут крайне важна и скорость расчетов, которую обеспечит биоэквайринг. Вместо среднестатистических 15 секунд весь процесс оплаты с помощью биометрии займет не более 5 секунд, уверяют в банке.

К слову, система «оплаты лицом» уже работает, но пока в качестве пилотного проекта. В частности, оплатить кофе лицом можно в кофейнях CoffeeBean. По прогнозам, в первую очередь биоэквайринг будет внедряться в магазинах, где важна скорость об-

служивания, да и не только в них.

«Сейчас уже многие клиенты по эквайрингу запрашивают информацию о внедрении биометрического способа оплаты товаров, услуг и счетов. Заинтересованы кафе, рестораны, ритейлеры и отели», — указывает председатель правления банка «Русский стандарт» Александр Самохвалов. — Это дает предприятиям возможность экономить, не увеличивая время обслуживания клиента, ведь в классическом эквайринге комиссии в два-три раза выше, чем в СБП. Мы планируем подключить к биометрическому платежу около десятка новых клиентов в конце 2019 — начале 2020 года».

Вас узнает банкомат

Еще одна новация — это обслуживание банкоматами по лицу. В частности, Сбербанк уже сейчас в качестве пилота запустил подобные банкоматы. На сегодняшний день пока система работает в тестовом режиме. Выглядит это так. Чтобы банкомат узнавал вас по лицу, необходимо единожды в нем верифицироваться (если биометрия уже сдана во внутреннюю биометрическую систему Сбербанка). Для этого нужно нажать клавишу «Обслуживание по биометрии», чтобы камера банкомата вас «узнала», потом с помощью банковской карты нужно полу-



МНЕ НУЖНЫ ТВОЕ ЛИЦО, ГОЛОС И КЛЮЧИ ОТ КВАРТИРЫ

АЛЕКСЕЙ ЛУКАЦКИЙ,
бизнес-консультант
по безопасности Cisco Systems

Биометрия — точная наука, в основе которой лежит мощный математический аппарат, который достаточно четко позволяет считать, насколько эффективным может быть биометрия в том или ином сценарии применения. В частности, существует две основных метрики — ошибки ложного обнаружения (false access rate, FAR) и ошибки ложного необнаружения (false

reject rate, FRR). В первом случае система утверждает, что человек, проходящий идентификацию, именно тот, за кого он себя выдает, хотя это не так, а во втором — человека просто не распознали, хотя его биометрические признаки в базе данных присутствуют. Показатели FAR и FRR часто указываются в материалах отдельных производителей (хотя для Единой биометрической системы таких цифр я не видел), но всегда возникает вопрос, кем и как они получены. Вариантов тут несколько. Самый простой — производитель сам провел тесты (а может, и не проводил, проверить-то нельзя) и сам их опубликовал. Вариант второй — провести тест на публичной базе биометрических признаков. В нем чуть больше независимости, но, так как объем таких баз не очень велик, всегда есть возможность, что производитель «заточит» свой алгоритм под конкретную базу данных, но в реальности его показатели будут гораздо хуже. Третий сценарий — участие в открытых конкурсах, например MegaFace. Ре-

зультаты будут еще надежнее, но и тут возможно подстроиться. Последний вариант — использование независимых тестов от независимой организации (в мире этим сегодня занимается NIST, американский институт стандартов и технологий) — лучше всего. Хотя и в нем есть свои подводные камни. В частности, мы не знаем, по какой базе NIST проводит тестирование. А это очень важно. В соцсетях у нас немало фотографий совершенно различного качества: есть паспортные фото (вы смотрите прямо в камеру, лицо на белом фоне, идеальные условия съемки), есть «селфи» неплохого качества с неоднотонным фоном и, возможно, повернутой головой, но чаще всего это фото, где лицо видно далеко не идеально. И вот тут очень важно понимать, какими изображениями будет оперировать система биометрии — как для своего обучения и хранения эталонных изображений лица, так и для идентификации. Одно дело, когда нас заставляют смотреть прямо в камеру с хорошим разрешением,

и совсем другое, когда нас снимают во время движения или с некачественным освещением. Результаты идентификации в этих двух случаях могут быть совершенно различными, причем в ситуации, когда человек не пытается скрыть свою личность. А что делать, если человек выдает себя за другого? Вы наверняка слышали про такое явление, как Deepfake, которое продемонстрировало, что сегодня любой желающий может с помощью бесплатного приложения в Apple AppStore или Google Play в шутку создать цифрового двойника любого известного человека. Но есть и более серьезные проекты, когда можно создать полноценную цифровую копию нужного нам человека, который говорит и движется так, как «жертва», у него та же мимика. Как системы биометрии борются с такими угрозами? Судя по тому, что совсем недавно компании Microsoft и Facebook запустили проект по распознаванию Deepfake, это очень серьезная проблема, которая пока не имеет решения.

Лично я бы с большим доверием стал относиться к таким проектам при соблюдении четырех условий: публичность данных об используемых решениях и их эффективности (указанием FAR, FRR и условий их получения). В том числе можно было бы говорить и о демонстрации работы биометрии в разных сценариях, для того чтобы снять опасения и недоверие к ней; правильное размещение видеокамер (для идентификации по лицу) для снятия изображений человека и повышения точности распознавания; четкое определение задачи для идентификации; наличие в массовых проектах команды для обслуживания, анализа, принятия решений. При эффективности биометрии на уровне 99,99% при большом объеме данных неизбежны ошибки. Кто-то должен разбираться со всеми этими кейсами. В противном случае я бы поостерегся от использования моей биометрии там, где без этого можно легко обойтись.

