УДК 336.71(045)

ИСПОЛЬЗОВАНИЕ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ И ПЕРСПЕКТИВЫ ЕЕ ПРИМЕНЕНИЯ В БАНКОВСКОЙ СИСТЕМЕ РОССИИ

ШАКЕР ИРИНА ЕВГЕНЬЕВНА,
канд. экон. наук, доцент Департамента финансовых рынков и банков Финансового университета
ish7@bk.ru

Статья посвящена идее использования банковских новаций в области биометрической аутентификации в России и за рубежом.
Цель работы — выявление основных проблем и направлений развития идентификации личности по голосу и внешности в условиях применения передовых инноваций, касающихся контактных и бесконтактных технологий.
Исследование позволило сделать следующие выводы: биометрические идентификационные технологии в России находятся на начальной стадии развития по сравнению с азиатскими или северо-американским рынками. Эффективных, готовых и апробированных наработок, которые можно было бы использовать в банковской системе России, пока нет ни у одного крупного банка. На развитие данного направления потребуется не один год. Основной задачей развития банковской системы в части биометрической аутентификации является ее перевод на «биометрические технологии», как планирует сделать Сбербанк, но пока рынок двигается в сторону развития персональных отношений клиента и банка посредством электронных технологий, в частности гаджетов.
Ключевые слова: банковский сектор; банковская платежная карта; идентификация; аутентификация; идентификация по голосу; идентификация по внешности; эффективность банковского бизнеса.

The Biometric Authentication and the Prospects for its Use in the Russian Banking System

SHACKER I.E.,
PhD (Economics), associate professor at the Financial Markets and Banks Department, Financial University
ish7@bk.ru

The paper describes the idea of using banking innovations for the biometric authentication in Russia and abroad. The purpose of the study was to identify the key problems and development trends in the identification of a person by voice and appearance in the context of using advanced innovations relating to contact and contactless technologies.
The study has led to the following conclusions: compared with the Asian and North American markets, biometric identification technologies in Russia are still in the infancy. So far, none of large banks has effective tried and tested technologies to be used in the Russian banking system. The development work in this area will take a number of years. The main goal of the banking system development in terms of biometric authentication is its switching to "biometric technologies" as Sberbank is planning to do, though in the meantime the market is moving in the direction of personal customer-to-bank relations through electronic technologies using various electronic gadgets.
Keywords: banking sector; bank payment cards; identification, authentication, voice identification, identification by appearance, (voice recognition and image recognition); the efficiency of the banking business.

Применение передовых технологий Сбербанком

Элементы предсказательной аналитики, искусственного интеллекта, сокращения сроков вывода продуктов на рынок, инвестиции в цифровые технологии выводят бизнес Сбербанка на передовые позиции. Число активных клиентов, которые владеют картами Сбербанка, достигло 120 млн, по всей стране установлено 86 тыс. банкоматов — это самая большая сеть банкоматов в мире, приложением «Сбербанк-Онлайн» пользуются 29 млн человек, число пользователей растет на 600–800 тыс. в месяц[1]. В условиях конкуренции и большого количества инновационных технологий банки уже сегодня задумываются о том, что необходимо сделать, чтобы в будущем они смогли соответствовать жестким условиям рынка и возрастающим требованиям клиентов. «Банки будущего» — это высокотехнологичные предприятия, использующие целый комплекс современных технологий для оптимизации работы, предоставления дополнительных сервисов клиентам и получения прибыли.

Банковская деятельность — одна из самых консервативных, однако внести в нее радикальные изменения способны технические новации. Высокие технологии изменяют содержание операций банка и позволяют добиваться конкурентного преимущества на рынке. Исходя из этого, очевидно, Г. Греф предположил[2], что Сбербанк введет в течение 2–3 лет новую систему идентификации клиентов с целью отказа банка от выпуска и использования платежных карт[3] и изменения потребности клиентов в банковских платежных картах[4].

Решения, которые предлагает Г. Греф: идентификация по голосу и внешности (*voice recognition u image recognition*) — нигде широко не применяются, то же самое касается и других видов биометрии — распознавания личности по ладони или отпечаткам пальцев[5].

Эксперты по банковскому рынку утверждают, что такой переход возможен, но не в течение 2–3 лет и только в качестве дополнительных мер обеспечения безопасности при осуществлении крупных сделок.

До настоящего времени в России функционировали только пилотные проекты. Так, в отдельных регионах держатели социальных карт ОАО «Сбербанк» могли оплачивать товары и услуги, сканируя отпечатки пальцев. Наиболее масштабно использует биометрическую идентификацию ОАО «Забсибком-банк». В его головном офисе и 24 филиалах установлена система *BioLink IDenium*. По отзывам службы информационной безопасности банка, внедрение этой системы обеспечило двойной эффект: усилило уровень информационной безопасности, минимизировало риски несанкционированного доступа и уменьшило затраты на решение инцидентов с паролями. Оценивая показатель *ROI*[6] от внедрения системы *IDenium* как высокий, руководство банка приняло решение о применении данной системы всеми филиалами [1, с. 17–21].

В созданном группой ВТБ банке «Лето» биометрические технологии применяются в процессе принятия и обработки кредитных заявок и основаны на системе сбора, хранения и использования в банковских процессах отпечатков пальцев клиентов. Банк «Хоум Кредит» начал внедрение биометрических технологий в 2011 г. Для этого была создана база фотографий клиентов. Как отмечает руководитель направления противодействия мошенничеству Ю. Лебединская-Литвинова, за 2011–2012 гг. финансовые вложения в биометрические технологии окупились, и был задержан 31 человек, подозреваемый в мошенничестве [1, с. 17–21].

---

[1] Сайт РБК. URL: http://www.rbc.ru/finances/27/05/2016/574835599a7947103afd8ece (дата обращения: 27 мая 2016 г.).

[2] Интервью газете «Известия»: Каледина А. Сбербанк опознает клиентов по голосу // Известия. URL: http://izvestia.ru/news/615407#ixzz49i6gIOwM.

[3] Там же. После внедрения платформы «18+», которое планируется к 2018 г., частота использования карты как инструмента платежа начнет резко снижаться.

[4] Каледина А. Сбербанк опознает клиентов по голосу // Известия. URL: http://izvestia.ru/news/615407#ixzz49i6gIOwM.

[5] Биометрические системы аутентификации — системы аутентификации, использующие для удостоверения личности людей их биометрические данные, проверка подлинности предъявленного пользователем идентификатора. Аутентификация требуется при доступе к таким интернет-сервисам, как электронная почта; веб-форум; социальные сети; интернет-банкинг; платежные системы; корпоративные сайты; интернет-магазины.

[6] *ROI* (от англ. *return on investment*) — финансовый коэффициент, иллюстрирующий уровень доходности или убыточности бизнеса, учитывая сумму сделанных в этот бизнес инвестиций.

Г. Греф также отмечает, что новая методика работы с клиентами затронет отделения Сбербанка за рубежом, но там могут возникнуть противоречия с международным правом.

По нашему мнению, если Сбербанк действительно захочет применить новые решения в своей практике, он создаст «замкнутый» продукт с неясной перспективой развития. Иными словами, интеграции с эквайринговыми сетями[7] биометрической технологии Сбербанка ожидать не приходится, трансграничные транзакции будут отключены, и во внутренней среде Сбербанк будет ограничен как минимум территориальными границами.

Однако никакой проблемы с введением подобной системы идентификации нет с правовой точки зрения. И пока это единственный положительный стимул для массового внедрения биометрии.

Угрозы неприкосновенности личности из-за накопления личной биометрической информации в компьютерных базах данных

Идея применения биометрии при оказании банковских услуг не является новой, футуристические прогнозы на эту тему делались еще в конце XX в., а серьезные работы, рассматривающие этот вопрос и носившие алармистский характер, появились в начале 2000-х гг. Верховный суд США отмечал наличие угрозы неприкосновенности частной жизни в накоплении личной биометрической информации в компьютерных базах данных или других массивах правительственных файлов. Угроза становится еще более реальной, учитывая расширение использования биометрических данных в коммерческих целях [2, с. 3–40].

До 1999 г. в США ни один федеральный или государственный орган не мог защитить биометрическую информацию от распространения в финансовых учреждениях. Только принятый акт Грэма — Лича — Блили — стандарта безопасности индустрии платежных карт — в какой-то мере решил данную проблему. Но только закон мог защитить биометрическую информацию об индивидууме, что и было сделано в штате Калифорния [2, с. 3–40].

В России нет правовых барьеров для осуществления биометрической идентификации в банковской сфере, но в то же время и нет законов, защищающих личные данные граждан. Для этого потребуется внести в законодательство изменения, касающиеся сбора и хранения биометрических данных в коммерческих целях.

Современные методы аутентификации клиента

Современные методы аутентификации клиента банка можно подразделить на три категории:

1) *то, что пользователь знает.* Этот метод основан на секретной информации, которую человек знает и применяет в целях аутентификации: пароль, ключевая фраза или персональный идентификационный номер (*PIN*);
2) *то, чем пользователь обладает*. Удостоверение личности, паспорт, банковская карта, *USB*-токен[8], различные ключи в других форматах — все это является примерами того, чем пользователь владеет и может использовать для своей идентификации;
3) *то, что есть сам пользователь*. Этот метод основан на физической или поведенческой особенности, которая является уникальной для человека и помогает его идентифицировать. Известными биометрическими методами аутентификации являются отпечатки пальцев, голос, сканирование радужной оболочки глаза, сканирование ладоней или геометрия руки, динамическая подпись [3, с. 67–78].

Мало кто сегодня сомневается в том, что в будущем будет осуществлен переход на третью группу методов аутентификации клиента в банковской сфере, и для этого есть весомые аргументы. Эффективность пароля зависит от секретности, которая может быть раскрыта посредством сниффинга[9], троянского коня, под-

[7] Эквайринг — оплата товара банковскими картами. Соответственно эквайринговая сеть — это сеть терминалов обычно банка (процессингового центра) в магазинах и т.д.

[8] *USB*-токен — компактное устройство, предназначенное для обеспечения информационной безопасности пользователя; также используется для идентификации его владельца, безопасного удаленного доступа к информационным ресурсам и т.д.

[9] Сниффинг (*sniffing*) — это перехват пакетов данных, передающихся между двумя компьютерами.

слушивания и слежения, социальной инженерии и т.д. Группа «*то, что пользователь знает*» относительно проста для проникновения. Чаще всего пользователи, чтобы не забыть или не ошибиться с паролем, записывают его на вещественные или электронные носители, что делает его уязвимым для кражи.

Известны пять уязвимостей в защите электронной информации, которые могут быть использованы с системами аутентификации на основе паролей и токенов:

1) клиент-атаки (брутфорс[10]);
2) хост-атаки (текстовые кражи и кражи кода доступа для токенов);
3) подслушивание, кража и копирование (подделка аппаратных средств для токенов);
4) ответ-атаки (ответ украденного пароля, ответ кода доступа);
5) троянский конь (установка вирусов на гаджеты клиента или удаленный захват устройства).

Биометрическая аутентификация обеспечивает естественное и наиболее надежное решение задачи распознавания личности. По причине того, что биометрические идентификаторы присущи только одному физическому лицу и никому другому, ими труднее манипулировать. Таким образом, биометрические признаки представляют собой сильную и достаточно постоянную связь между человеком и его личностью. Но голос может меняться из-за болезни, возраста, со временем изменяется и внешность человека.

Разумеется, в научных кругах дискутируется вопрос о возможной фальсификации биометрических признаков посредством, например, репликации отпечатков пальцев. После того как информация фиксируется, отпечатки (или другие биометрические характеристики) трансформируются в оцифрованные данные, которые могут быть сымитированы. Если преступники способны создать «копию» данных, они могут представляться в банке как лицо, которому принадлежат эти данные. Кроме того, одна из причин, почему в развитых странах биометрическая аутентификация не принимается в широком масштабе, — это необходимость соблюдения строгих правил по защите персональных данных, таких как Европейское положение о защите данных (*GDPR*) [4, с. 9152–9160].

Риск компрометации биометрической информации, хранящейся в централизованной базе данных, является реальным и неприемлемым для безопасности многих государств в целом и для банков в частности. Отсюда проистекают жесткие ограничения по международному взаимодействию в этой сфере.

Интересной выглядит и идея сделать упор на идентификацию голоса и внешности, учитывая, что в мире наибольшее распространение получают технологии, связанные с распознаванием отпечатков пальцев, и не в последнюю очередь это связано с применением подобных технологий в смартфонах и других гаджетах. Именно аутентификация посредством отпечатка является наиболее распространенной и в общем объеме биометрическая аутентификация занимает 48,8% от всех операций с биометрией, тогда как голосовое сканирование — 4,3%, сканирование лица — 15,4%, а сканирование ладони — 10,4% [5, с. 67–78].

Биометрическая аутентификация обеспечивает естественное и наиболее надежное решение задачи распознавания личности

В настоящее время биометрические технологии в основном внедряются в интернет-торговлю. Одной из основных проблем, связанных с аутентификацией пользователей через Интернет, является отсутствие обеспечения безопасности у традиционных методов аутентификации: данных карты, пароля, *cvc*-кода[11] — все это может попадать в файлы-*cookie* и быть считанным по незащищенным соединениям. При нынешнем состоянии развития биометрического рынка технологий снятия отпечатков пальцев возможность идентификации индивидуума в Интернете

[10] Брутфорс (от англ. *brute force*) — полный перебор или метод «грубой силы» — один из популярных методов взлома паролей на серверах и в различных программах.

[11] Код проверки подлинности карты (от англ. *card verification value*).

становится более адресной. Биометрическая система аутентификации отпечатков пальцев стала одним из решений, позволяющим включать проверку личности клиента с использованием объектов, встроенных в веб-страницы [6, с. 7].

Использование биометрии в банковском бизнесе

При анализе деятельности 121 мирового банка в 2012 г. был сделан вывод о том, что отпечатки пальцев являются самой популярной биометрической технологией. Новые исследования, проведенные в отношении уже 184 банков из 35 стран, дали тот же результат [6, с. 7].

Ученые отмечают, что факторами, замедляющими распространение биометрии, являются очень высокая стоимость ее применения и неопределенность, связанная со стандартами, регламентирующими ее использование. Банки вынуждены вкладывать средства в дорогостоящие технологии биометрии, в то время как мир нуждается в простоте и технологичности.

На основании вышеприведенного можно сделать вывод, что попытка создания Сбербанком собственной локальной системы работы с биометрическими данными выглядит не совсем реалистичной, тем более в условиях, когда весь мир будет унифицировать эту работу, стараясь отказываться от дорогостоящего оборудования, передавая функцию сбора информации гаджетам потребителей.

Проекты и прогнозы развития

Несмотря на неопределенность относительно того, как биометрический рынок будет развиваться в ближайшие годы, можно, по нашему мнению, ожидать позитивных изменений. Например, прогнозируется, что к 2020 г. биометрия будет использоваться для аутентификации почти 65% сделок мобильной коммерции через приложения, загруженные самими потребителями. Согласно другим оценкам объем рынка глобальных биометрических технологий будет равняться 22 млрд долл. США к 2020 г. [7, с. 1].

Биометрия в банковском деле наиболее популярна в развивающихся странах Азии, таких как Индия и Индонезия — на этот континент приходится 52% банковских операций с использованием биометрических данных. Америка занимает второе место с 32%, далее следуют Европа (9%), Африка (6%) и Австралия (1%). В Японии поддерживается сеть из более чем 80 тысяч биометрических банкоматов, которыми пользуются более 15 млн клиентов [7, с. 3].

Попытка создания Сбербанком собственной локальной системы работы с биометрическими данными выглядит не совсем реалистичной

Финансовые учреждения и регулирующие органы в странах с развитой экономикой проявляют осторожность при внедрении биометрической аутентификации, что вызвано предполагаемыми утечками информации из централизованных баз данных, которые могут быть разрушительными для рынка, особенно если нарушается безопасность трансграничных операций.

Рассмотрим развитие биометрических технологий в банковской сфере на конкретных примерах. Банк *HSBC* начинает внедрение распознавания голоса и сенсорных услуг по использованию *ID*[12] для 15 млн клиентов и предполагает запустить этот проект в 2016 г., что станет самым масштабным внедрением биометрических технологий в коммерческой сфере для Великобритании[13].

Клиенты банка *HSBC* смогут использовать телефонный банкинг и мобильное приложение, чтобы получить доступ к своим счетам посредством системы передачи голоса и отпечатков пальцев. Банк тем самым надеется, что программное обеспечение поможет решить проблему забытых или украденных паролей и голосовых технологий биометрической безопасности в Великобритании. Запуск голосовой и сенсорной идентификации делает получение доступа к своим банковским счетам более быстрым и

[12] *ID* — это уникальный номер, который присваивается каждому пользователю для его идентификации.

[13] Julia Kollewe HSBC rolls out voice and touch ID security for bank customers // The Guardian. URL: https://www.theguardian.com/business/2016/feb/19/hsbc-rolls-out-voice-touch-id-security-bank-customers.

простым для клиентов, использующих наиболее безопасный вид технологии пароля — свое собственное тело[14].

Банк *Barclays* представил программное обеспечение распознавания голоса для всех своих 300 тыс. наиболее богатых клиентов в Великобритании в 2013 г. Через год руководство банка заявило, что технология была настолько успешной, что она будет внедрена для всех 12 млн розничных клиентов банка. Но реализация проекта затянулась, планы по внедрению всеобщей системы решили перенести на конец 2016 г.[15]

В США ряд банков также экспериментировал с биометрическими технологиями. *Citibank* насчитывает около 250 000 клиентов, которые используют голосовые технологии для аутентификации. Но, как показала практика, многих людей совсем не интересуют новые технологии, даже если они предоставляются банком. Массовый опрос клиентов банков в 2015 г., осуществленный газетой *American Banker*, показал, что многие даже не подозревают о цифровых технологиях, предлагаемых их банком, в том числе использование сенсорного *ID* на их телефонах *Apple*. В то же время оказалось, что многие потребители были бы рады ввести имя пользователя и пароль, чтобы чувствовать себя более безопасными[16].

В *Citibank* действует следующая схема: клиенты, которые хотят воспользоваться преимуществами аутентификации голосом, сначала предоставляют краткий голосовой образец. *Citibank* работает с *NiceSystems*[17] по технологии, способной идентифицировать около 130 различных характеристик голоса человека, что позволяет опознать звонящего. Немногим больше трети крупных американских банков заявили, что биометрическая технология будет приоритетом для них в ближайшие годы согласно исследованию, проведенному лондонской компанией *Ovum*.

Такие технологии, как сканирование лица или аутентификация клиента по голосу, будут становиться все более популярными, так как поколение Зет предпочитает именно такие способы взаимодействия с внешней средой при получении услуг. Опрос 1000 молодых людей показал, что в идентификации себя с помощью мобильных устройств 61% респондентов предпочитают отпечатки пальцев. Кроме того, почти треть опрошенных заявили, что они были бы рады внедрению технологий по распознаванию лица[18].

Однако до настоящего времени эксперты по американскому банковскому рынку серьезно не рассматривают варианты по переводу банкоматов на работу с биометрией, так как не видят в этом больших преимуществ перед использованием классической банковской карты, учитывая издержки таких масштабных перемен. Большинство склоняется к тому, что развитие биометрических технологий в банковской сфере в краткосрочном периоде релевантно только для удаленных услуг, например работы с личным кабинетом или интернет-платежей.

Основываясь на данных опроса, проведенного компанией *Unisys*, являющейся одним из ведущих поставщиков биометрических решений, можно сделать вывод, что в Великобритании сегодня 56% потребителей не возражают против предоставления биометрических данных в целях установления личности при совершении розничных покупок и финансовых транзакций, 95% британцев готовы к этому (а также к сканированию отпечатков пальцев) при работе с банками и государственными службами. Количество граждан в развитых странах, готовых применять биометрию, колеблется от 50% в Германии до 66% в Австралии. Сканирование отпечатков пальцев стало сегодня наиболее широко распространенным биометрическим методом, оставляя позади сканирование лиц и анализ голоса [8, с. 102–110].

---

[14] Julia Kollewe HSBC rolls out voice and touch ID security for bank customers // The Guardian. URL: https://www.theguardian.com/business/2016/feb/19/hsbc-rolls-out-voice-touch-id-security-bank-customers.

[15] Там же.

[16] Bryan Yurcan Banks Embrace Biometrics, But Will Customers? // American Banker: Banking & Financial News. URL: http://www.americanbanker.com/news/bank-technology/banks-embrace-biometrics-but-will-customers-1078867-1.html.

[17] *Nice Systems Ltd.* — израильская *high-tech* компания, один из лидеров в области проектирования и поставки центров для бизнес-контактов, записи телефонных и видеоразговоров, биржевых операций и управления воздушным движением.

[18] Bryan Yurcan Banks Embrace Biometrics, But Will Customers? // American Banker: Banking & Financial News. URL: http://www.americanbanker.com/news/bank-technology/banks-embrace-biometrics-but-will-customers-1078867-1.html.

Необходимо также отметить, что данная инновация представляется чрезвычайно затратной, и такие варианты развития работы с клиентами не рассматриваются ни одним крупным западным банком, ограничиваясь применением биометрических технологий только для удаленной работы.

Банковские карты рано или поздно отомрут, и ни у кого не возникает сомнений на этот на счет. Но это займет много времени. Так, впервые рынок увидел карточный чип в 1988 г., но самые оптимистичные прогнозы относительно перехода большинства развитых стран на смарт-карты относятся только к 2018 г., т.е. через 30 лет после появления данной технологии.

Выводы

Биометрические идентификационные технологии находятся в России на начальной стадии. Готовых инновационных технологических решений пока нет. Поэтому на развитие этого направления вплоть до его промышленного внедрения уйдет примерно столько же времени, сколько заняла реализация проектов по внедрению биометрической идентификации в развитых западных странах.

Внедрение биометрии в практику работы банков может стать успешной альтернативой методу удаленного подтверждения операций с помощью одного лишь кодового слова или оглашения паспортных данных в качестве дополнительного механизма при многофакторной аутентификации клиента. Биометрическая идентификация имеет большое будущее в плане развития персональных отношений клиента и банка с помощью гаджетов, а не в плане перевода банковской сети на «биометрические рельсы», что замышляет Сбербанк.

Учитывая все большее смещение применения биометрии в сторону розничной интернет-торговли и работы с мобильными приложениями, можно утверждать, что для корпоративных клиентов в среднесрочной перспективе данные технологии станут лишь дополнительным методом аутентификации, но они никак не изменят архитектуру взаимоотношений клиентов с банками.

Литература (references)

1. Гришина Е.А. Биометрические технологии в российских банках: мечты или реальность // Наука и общество. 2015. № 3. С. 17–21.
   Grishina E.A. Biometric Technologies in Russian banks: dream or reality [Biometricheskie tehnologii v rossijskih bankah: mechty ili real'nost']. *Nauka i obshhestvo — Science and Society,* 2015, No. 3, pp. 17–21.
2. Lisa McGuire Banking on biometrics: your bank's new high-tech method of identification may mean giving up your privacy. *Akron Law Rewiew*, 2000, No. 33, pp. 3–40.
3. Gunajit Sarma Internet Banking: Risk Analysis and Applicability of Biometric Technology for Authentication. *International Journal of Pure and Applied Sciences and Technology,* 2010, No. 1, pp. 67–78.
4. Seyyede Hosseini Review Banking on Biometric in the World's Banks and Introducing a Biometric Model for Iran's Banking System. *Journal of Basic and Applied Scientific Research,* 2012, No. 3, pp. 9152–9160.
5. Gunajit Sarma Internet Banking: Risk Analysis and Applicability of Biometric Technology for Authentication // *International Journal of Pure and Applied Sciences and Technology*, 2010, No. 1, pp. 67–78.
6. Biometrics for payments. *New science: transaction security*. UL New Science newscience.ul.com/NS TS Article 2014. p. 7.
7. Nathaniel Karp Biometrics: The Future of Mobile Payments. *U.S. Economic Watch.* 20 July 2015, p. 1.
8. Рудская Е.Н. Биометрические инструменты для бизнеса // Актуальные вопросы современной науки. 2013. № 30. С. 102–111.
9. Rudskaya E.N. Biometric tools for businesses [Biometricheskie instrumenty dlja biznesa]. *Aktual'nye voprosy sovremennoj nauki — Actual problems of modern science,* 2013, No. 30, pp. 102–111.