

Моногарова А. А., студент бакалавриата 2 курс, финансово-экономический факультет/департамент корпоративных финансов и корпоративного управления, Финансовый университет при Правительстве Российской Федерации, Москва

Курзанов И. Д., студент бакалавриата 2 курс, финансово-экономический факультет/департамент корпоративных финансов и корпоративного управления, Финансовый университет при Правительстве Российской Федерации, Москва

Николайчук О. А., научный руководитель, д.э.н. профессор департамента экономической теории, Финансовый университет при Правительстве Российской Федерации, Москва

БИОМЕТРИЯ КАК СПОСОБ УДАЛЁННОЙ ИДЕНТИФИКАЦИИ В БАНКОВСКОМ СЕКТОРЕ

Аннотация: В статье ставится задача рассмотреть перспективы применения биометрии в российском банковском секторе. В статье анализируется международный и российский опыт внедрения биометрии. Выявлены проблемы и возможные угрозы её применения.

Ключевые слова: биометрия, удалённая идентификация, интернет-банкинг, персональные данные, цифровая экономика.

Abstract: The article sets the task to consider the prospects of using biometrics in the Russian banking sector. The article analyzes the international and Russian experience in implementing biometrics. The problems and possible threats of its application are identified.

Keywords: biometrics, remote identification, Internet banking, personal data, digital economy.

В данной работе мы рассмотрим место биометрии в процессе становления цифровой экономики. Актуальность выбранной темы обуславливается активным переходом к цифровой экономике, а также её поддержкой со стороны Правительства и Центрального Банка.

Удаленная идентификация — это механизм, позволяющий физическим лицам получать финансовые услуги дистанционно в разных банках, подтвердив свою личность с помощью биометрических персональных данных (изображение лица и голос) [5]. Биометрия – это составляющая удаленной идентификации, включающая в себя набор различных измеренных параметров человека для его дальнейшей идентификации, так как данный набор уникален

для каждого человека. Всё это – один из многих инструментов необходимых для становления цифровой экономики.

В целях развития цифровой экономики создаётся информационная инфраструктура и появляются новые нормативно-правовые акты. Основная программа носит название «Цифровая экономика», в рамках которой планируется увеличение производительности труда с помощью новых технологий на 30% к 2024 году. В частности, были внесены правки в закон "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" и была создана единая биометрическая система – система сбора, обработки, хранения персональных биометрических данных, которая осуществляет проверку биометрических данных и их соответствие тем, что были предоставлены ранее.

Все технологические изменения и повлёкшие их новые нормативные акты в совокупности могут в корне поменять банковскую систему в ближайшие годы. Как крупные, так и малые банки смогут снизить свои издержки, а, следовательно, это поможет более мелким игрокам увеличить свою долю рынка, что сильно скажется на конкуренции, которая будет способствовать развитию финансового рынка в целом. Цифровизация скажется как на повышении доступности услуг, так и на их качестве, так как это не просто локальное снижение издержек, а целое изменение конъюнктуры финансового рынка. Но все это невозможно без средств защиты и на «передовой» тут находится биометрическая идентификация.

Российский рынок биометрии в более динамичной стадии развития, чем мировой, благодаря инициативам, описанным выше, и уже идущей форсированной интеграции биометрии в банковский сектор. По прогнозам до 2022 года ежегодные темпы роста в нашей стране превысят общие показатели по миру приблизительно в 1,5 раза (рис. 1) [6].

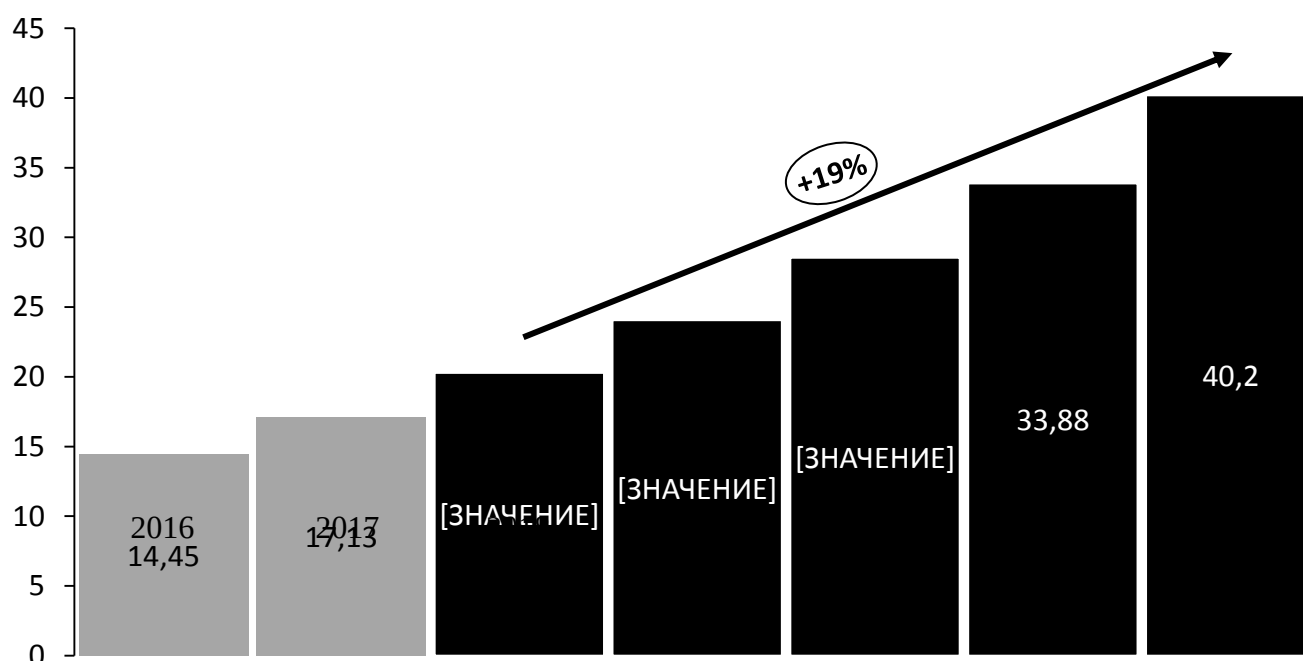


Рисунок 1 - Объем мирового рынка биометрических систем 2016-2022 гг., млрд долл. США

На данный момент доступ в единую биометрическую систему осуществляется на бимодальной основе: по верификации голоса и лица. В ходе проверки результаты двух проверок обобщаются. Аутентификация по голосу и лицу является наиболее оптимальной, так как она не требует специального оборудования и её можно осуществить со смартфона или компьютера, что удобно для широкого круга пользователей [8, с. 6].

Центральный Банк обязал банки с универсальной лицензией предоставлять услуги с использованием удалённой идентификации к сентябрю 2020 года [5]. В целях выполнения указания российские банки Сбербанк и Тинькофф уже закупили десять тысяч биометрических банкоматов, которые планируется внедрить до конца 2019 года. Сейчас процесс сдачи биометрии остаётся не очень удобным для клиента, поэтому банки пытаются оптимизировать процесс, так, в Сбербанке можно сдать данные через смартфон, позже подтвердив их либо звонком в коллцентр, либо придя в отделение. Центральный банк предоставляет банкам, собирающим биометрию, льготы в виде снижения ставки резервирования по кредитам, выданным с помощью биометрии. Тем не менее, все расходы, связанные с установлением

оборудования, несут на себе банки, что не сильно уменьшит процент по биометрическим кредитам.

Сейчас, чтобы получить доступ к удалённой идентификации посредством биометрии, достаточно в пункте сдачи произнести цифры от 0 до 9 в прямом, обратном и случайном порядке, а также сделать фотоизображение с полным фронтальным изображением лица согласно ГОСТу Р ИСО/МЭК 19794-5-2013 [7]. В течение пяти дней после сдачи данных учётная запись будет активирована и будет возможно открыть счёт, вклад или оформить кредит удалённо. В будущем ожидается появление других банковских и небанковских услуг, к которым можно получить доступ, используя биометрические данные, это, вместе с тем, что при сдаче биометрии требуется подтверждённый аккаунт на Госуслугах, ставит под сомнение конфиденциальность данных при передаче их другим ведомствам. Более того, сам Центральный Банк усматривает угрозу на всех этапах сбора, обработки и передачи данных. Это могут быть подмена сканирующих устройств, копирование биометрического материала, а также перехват сигнала при передаче биометрических данных [4, с. 235].

На международной арене эксперименты с внедрением биометрической идентификации проводятся относительно давно. Так Lloyds Banking Group plc, являющаяся одним из крупнейших финансовых учреждений, обслуживающих как бизнес, так и частных лиц, заключила партнерские отношения с Microsoft, чтобы позволить своим клиентам войти в свои банковские сервисы и подтвердить подлинность транзакции с помощью распознавания отпечатков пальцев и распознавания лиц. Пользовательские биометрические данные зашифрованы и хранятся локально, чтобы защитить их от любого неправомерного использования. Также Lloyds модернизировали свою цифровую безопасность с помощью технологии многофакторной аутентификации от Callsign.

В 2017 году MasterCard представили свою карту с датчиком для считывания отпечатка пальца. Процедура аутентификации выглядит похожей на оплату через ApplePay или SamsungPay, в случае несовпадения отпечатка на

сканере и на чипе, система просит ввести PIN [3]. Также MasterCard объявили, что запускают «Selfie Pay» – новый метод для подтверждения своей личности при совершении транзакций в Интернете. Обновление позволяет владельцам карт удостоверить свою личность, используя биометрические данные, такие как отпечатки пальцев или распознавание лиц – последнее требует, чтобы пользователи делали «селфи». Цель этого шага – отодвинуть потребителей от менее защищенной природы паролей. Согласно исследованиям Mastercard, девять из десяти человек, которые были протестированы в ходе голландского пилота, заявили, что хотели бы окончательно заменить свой пароль биометрической идентификацией, в то время как 75% пользователей сказали, что они убеждены, что биометрические платежи уменьшат мошенничество. Вслед за пилотом 93% пользователей заявили, что они с радостью продолжают использовать распознавание отпечатков пальцев, а 77% заявили, что с удовольствием используют распознавание лиц для завершения своих платежей.

Финансовая группа Sumitomo Mitsui, одна из крупнейших финансовых групп Японии, вместе со своими технологическими партнерами NTT Data и Daon разработали Polarify – сервис, который обеспечивает безопасную и удобную биометрическую аутентификацию в нескольких каналах и правила e-KYC («знай своего клиента») для упрощенной цифровой регистрации. Polarify быстро стал привлекательной альтернативой, предлагая лучшие в своем классе возможности биометрической аутентификации и регистрации в качестве услуги на рынке Японии. С помощью приложения Polarify можно получить не только банковские услуги, партнёрами проекта также выступили некоторые из самых престижных компаний в области электронной коммерции и страхования, в том числе крупнейшая японская компания по страхованию жизни [2].

Nationwide запустили поведенческую биометрию для своих клиентов в Великобритании, добавив совершенно новый уровень к «персонализированному опыту работы с клиентами». HSBC теперь предлагает распознавание голоса. Atom Bank, один из крупнейших цифровых банков Великобритании, запустил цифровое банковское приложение, которое

использует биометрические данные лица и голоса, чтобы пользователи могли войти в свой аккаунт.

Эти нововведения усиливают понятие безопасности, и потребители начинают рассматривать такие меры безопасности как «норму». Стоит отметить, что ни в одной стране, кроме России, не была создана единая централизованная база биометрических данных. Все нововведения за рубежом были внедрены частными компаниями.

Принимая во внимание риски и угрозы, возникающие при идентификации и аутентификации клиентов банка с использованием их биометрических данных, следует понимать, что они возникают на каждом этапе идентификации или аутентификации, с момента сбора биометрических данных до их завершения с окончательным доступом. Важной проблемой на данный момент остается вопрос безопасности, так как при таком активном росте рынка будет также активно увеличиваться количество мошенников. Возможные способы взлома еще не были изучены до конца, так как постоянно появляются новые угрозы. Мошенники постоянно придумывают, как обойти меры защиты, и системы безопасности приходят в негодность, из-за чего производителям данных систем придется постоянно играть в «кошки мышки» с взломщиками, чтобы обеспечить наивысшую безопасность пользователям. Однако, финансовый рынок, в частности банковский, не может себе позволить даже временного отставания от злоумышленников, что на данный момент ставит под сомнение использование биометрии на государственном уровне, так как биометрия это не пароль и не ПИН-код, ее нельзя поменять: если произошла утечка, то все жертвы больше не смогут безопасно использовать ее, а следовательно она становится для них бесполезна. Даже инновационные меры защиты в виде создания 3D объемных моделей лица человека, чтобы мошенники никак не могли пройти проверку, используя фотографию, можно обойти благодаря полноценному моделированию по одной фотографии лица человека, что легко реализуемо из-за алгоритма прямой регрессии объемного представления трехмерной геометрии лица из одного 2D-изображения [1].

Таким образом, можно сделать вывод, что на этом этапе развития технологий биометрические данные должны использоваться как часть многофакторной идентификации, например, в сочетании с классическими видами аутентификации, например, паролями, чтобы минимизировать последствия компрометации данных.

Поскольку сами технологии все еще появляются, часто именно их внедрение, а не сами технологии, приводит к уязвимостям безопасности. В целом известно, что, несмотря на кажущуюся точность биометрии, ложные срабатывания (FAR) и ложные отказы (FRR), блокирующие легитимный доступ или разрешающие нелегитимный доступ, всё ещё возможны.

Децентрализованная база данных, создаваемая и шифруемая отдельно каждым банком, более оптимальна, так как при взломе данных одного банка счета клиента в других банках не страдают.

В связи с расходами на установку оборудования ставки по биометрическим кредитам не будут снижены достаточно ощутимо для того, чтобы компенсировать страх клиентов, связанный с утечкой и недобросовестным использованием данных.

Библиографический список:

1. 3D Face Reconstruction from a Single Image: online demo of paper Large Pose 3D Face Reconstruction from a Single Image via Direct Volumetric CNN Regression [Электронный ресурс]. – Режим доступа: <http://cvl-demos.cs.nott.ac.uk/vrn> (дата обращения: 20.12.2019).
2. Case study: Polarify - joint venture for cross channel biometric authentication and E-KYC [Электронный ресурс]. – Режим доступа: <https://www.daon.com/resources/case-studies/polarify> (дата обращения: 10.12.2019).
3. Mastercard is developing the next generation solution to provide cardholder security using biometrics. [Электронный ресурс]. – Режим доступа:

<https://www.mastercard.us/en-us/merchants/safety-security/biometric-card.html> (дата обращения: 15.12.2019).

4. Григорян А. С. Идентификация и аутентификация клиентов банков посредством биометрии и сопутствующие угрозы // Конф. "Социально-экономические и гуманитарные науки". "Технические и естественные науки". "Образование. Культура. Общество" / Частное научно-образовательное учреждение дополнительного профессионального образования Гуманитарный национальный исследовательский институт «НАЦРАЗВИТИЕ» – СПб., 2019. – С. 232 – 338.

5. Информация Банка России «Основные направления развития финансовых технологий на период 2018-2020 гг.» [Электронный ресурс]. – Режим доступа: https://www.cbr.ru/Content/Document/File/84852/ON_FinTex_2017.pdf (дата обращения: 15.12.2019).

6. Исследование российского рынка биометрических технологий 2018-2022 гг. Компания J'son & Partners Consulting [Электронный ресурс]. – Режим доступа: http://json.tv/ict_telecom_analytics_view/issledovanie-rossiyskogo-rynka-biometricheskih-tehnologiy-2018-2022-gg-20181130015609 (дата обращения: 14.12.2019).

7. Методические рекомендации по нейтрализации банками угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации (утв. Банком России 14.02.2019 N 4-МР).

8. Симончик К.К., Белевитин Д.О., Матвеев Ю.Н., Дырмовский Д.В. Доступ к интернет-банкингу на основе бимодальной биометрии// Мир измерений – 2014 – №3 – с. 6-10.