УДК 2964 JEL O14 *DOI 10.26425/1816-4277-2020-5-193-199*

Шаманина Елизавета Ивановна
канд. экон. наук, ФГБОУ ВО «Государственный университет управления», г. Москва, Российская Федерация
ORCID: *0000-0001-5777-5323*
e-mail: *shamanina_ei@mail.ru*

Захаренко Юлия Сергеевна
студент, ФГБОУ ВО «Государственный университет управления», г. Москва, Российская Федерация
ORCID: *0000-0002-0662-5285*
e-mail: *yulia_zakharenko@mail.ru*

БИОМЕТРИЧЕСКИЕ ТЕХНОЛОГИИ КАК ПЕРСПЕКТИВНОЕ НАПРАВЛЕНИЕ СОВЕРШЕНСТВОВАНИЯ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

Аннотация. *Рассмотрены вопросы, связанные с развитием и совершенствованием в российском банковском секторе механизма удаленной идентификации. Освещены основные аспекты процесса сбора, обработки, проверки и хранения биометрических данных, статус функционирования единой биометрической системы (ЕБС). Отмечены уязвимость и риски применения банками биометрических технологий. Представлены ключевые тренды развития международного рынка биометрических технологий и их применение в банковском секторе, а также актуальные мероприятия по внедрению биометрических технологий в России. Обозначены перспективы использования биометрических технологий в банковском секторе и направления совершенствования технологической инфраструктуры в целях защиты данных от несанкционированного доступа.*

Ключевые слова: *биометрические персональные данные, сбор, обработка, проверка, хранение данных, удаленная идентификация, единая биометрическая система, ЕБС, биометрические технологии, дорожная карта внедрения биометрии, дистанционное банковское обслуживание, риски.*

Цитирование: Шаманина Е.И., Захаренко Ю.С. Биометрические технологии как перспективное направление совершенствования дистанционного банковского обслуживания//Вестник университета. 2020. № 5. С. 193–199.

Shamanina Elizaveta
Candidate of Economic Sciences, State University of Management, Moscow, Russia
ORCID: *0000-0001-5777-5323*
e-mail: *shamanina_ei@mail.ru*

Zakharenko Yulia
Student, State University of Management, Moscow, Russia
ORCID: *0000-0002-0662-5285*
e-mail: *yulia_zakharenko@mail.ru*

BIOMETRIC TECHNOLOGIES AS A PERSPECTIVE DIRECTION OF IMPROVING REMOTE BANK SERVICE

Abstract. *The issues related to the developing and improving remote identification mechanism in the Russian banking sector have been considered. The main aspects of the process of collecting, processing, checking and storing biometric data, the functioning status of Single Biometric System (SBS) have been highlighted. The vulnerability and risks of using biometric technologies by banks have been noted. The key trends in the development of the international market of biometric technologies and their application in the banking sector have been presented, as well as current events on the implementation of biometric technologies in Russia. The prospects for the use of biometric technologies in the banking sector and directions for improving the technological infrastructure in order to protect data from unauthorized access have been outlined.*

Keywords: *biometric personal data, collecting, processing, checking, storing data, remote identification, single biometric system, SBS, biometric technologies, biometrics implementation roadmap, remote bank service, risks.*

For citation: Shamanina E.I., Zakharenko Yu.S. (2020) Biometric technologies as a perspective direction of improving remote bank service. *Vestnik universiteta*. I. 5, pp. 193–199. DOI: 10.26425/1816-4277-2020-5-193-199

В настоящее время банки активно продолжают развивать сервисы и каналы дистанционного банковского обслуживания (далее – ДБО) как наиболее перспективные и эффективные способы взаимодействия с клиентами, обеспечивающие удобство доступа к банковским продуктам и услугам, и быстроту совершения операций. В свою очередь, проблемы реализации банковских продуктов и услуг в удаленных каналах, связанные с ограничениями технологического характера, постепенно исчезают. Помимо удобства и экономии времени, современные системы ДБО отвечают таким требованиям, как высокая производительность, надежность и безопасность.

Развивая и совершенствуя возможности ДБО, банки также активно прорабатывают вопросы, связанные с повышением безопасности удаленных каналов.

Можно отметить, что сейчас одним из ярких и перспективных трендов в области удаленной идентификации и авторизации клиентов являются биометрические технологии.

Активному внедрению биометрических технологий на российском банковском рынке способствовало принятие в декабре 2017 г. Федерального закона № 482-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации», согласно которому банки могут дистанционно открывать счета (вклады), предоставлять кредиты и осуществлять переводы без личного присутствия клиента, используя его биометрические данные и данные Единой системы идентификации и аутентификации (далее – ЕСИА) [2].

Согласно статье 11 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»,«биометрические персональные данные – это сведения, которые характеризуют физиологические и биологические особенности человека, с помощью которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных» [1].

Итак, какие же параметры человека можно отнести к биометрическим персональным данным? Во-первых, это данные, которые характеризуют физиологические и биологические качества человека, такие как отпечатки пальцев, скан руки, ДНК-анализ, рисунок радужки глаза, рисунок вен, голос, распознавание лица. Во-вторых, к биометрическим данным также относятся отдельные факторы, характеризующие поведение человека в тех или иных ситуациях.

Но есть и такие данные, которые не могут подтвердить личность человека, то есть не являются биометрическими. К ним можно отнести следующие: фотография, подпись человека, почерк, рентгеновские или флюорографические снимки, материалы видеосъемки с камер наблюдения в публичных местах и на охраняемых территориях.

В целях эффективного сбора, использования, хранения и систематизации собранных биометрических данных в России создана Единая Биометрическая Система (далее – ЕБС) – информационная база, в которой хранятся все биометрические данные российских граждан. Она начала свою работу 1 июля 2018 г., ее разработчиком и главным оператором выступил Ростелеком, который обрабатывает данные и обеспечивает их безопасное хранение [14].

Стоит заметить, что с 2018 г. начали прием биометрии несколько крупных банков – Сбербанк, ВТБ, Альфа-Банк, Райффайзенбанк, Почта Банк. Сейчас каждый гражданин России может сдать запись своего голоса и изображения лица, чтобы пополнить данные ЕБС. По этим данным можно идентифицировать личность человека в отделении банка, по телефону или через приложение «мобильный банк».

В будущем биометрическая система должна облегчить работу банков, упростить и ускорить процесс предоставления клиентам финансовых услуг. Так, для определения личности клиента предоставление паспорта станет необязательной процедурой, достаточно будет сопоставить голос и лицо человека с имеющимися в базе записями для идентификации личности. Благодаря этому клиенты банка смогут оформить любой продукт в удобное время, в любом месте, по телефону или через интернет-банк.

Еще одним перспективным трендом внедрения биометрических технологий является развитие взаимодействия ЕБС и ЕСИА в целях предоставления доступа к порталу Госуслуг. В дальнейшем доступ к данным в ЕБС планируется предоставить отдельным государственным структурам, например, полиции, чтобы облегчить поиск правонарушителей, и учреждениям здравоохранения для улучшения систематизации медицинской базы [10].

Каким образом происходит процесс сдачи биометрических персональных данных? На сайте Банка России размещена карта, с помощью которой можно узнать какие отделения банков принимают биометрические данные, их адреса и время работы.

На практике процесс сдачи биометрических данных в отделении Сбербанка (например, при плановой замене банковской карты) выглядит следующим образом. Во время выдачи карты сотрудник банка обращается к клиенту с предложением сдать персональные биометрические данные в целях повышения степени защиты личных клиентских данных, а также облегчения процесса взаимодействия с банком и подписать соответствующее согласие на обработку персональных данных.

Непосредственно сам процесс сдачи биометрии включает 2 этапа:

– клиенту предлагается произнести вслух цифры – от 0 до 9, а затем от 9 до 0, и в случайном порядке;
– сотрудник банка производит фотосъемку лица клиента крупным планом.

После внесения биометрических данных в ЕБС (голос и изображение лица) на мобильный телефон клиента направляется смс-уведомление с подтверждением внесения персональных биометрических данных в базу. Далее, чтобы воспользоваться биометрией для получения банковского продукта или услуги, клиенту необходимо указать свой логин и пароль в ЕСИА, произнести кодовое слово и показать в камеру свое лицо. Система самостоятельно сопоставит данные с имеющимися образцами, после чего сообщит о результатах проверки. Если они совпадут, то банк продолжит оформление продукта или услуги, а всю необходимую персональную информацию банк загрузит из ЕСИА. Таким образом, становясь участником данного процесса, банк обязан взаимодействовать с ЕБС и ЕСИА для передачи биометрических данных клиентов.

Действующий в России механизм двухуровневого хранения данных, предусматривающий хранение идентификационных персональных данных (ФИО, реквизиты паспорта, СНИСЛС и др.) в ЕСИА, а биометрических (образцы голоса и изображения лица) в ЕБС, предоставляет дополнительные гарантии защиты персональных данных. При этом важным моментом в контексте минимизации рисков мошеннических действий является условие хранения биометрических данных в обезличенной форме без их привязки к персональным данным.

Таким образом, использование биометрических технологий позволяет минимизировать риски, связанные с возможным хищением средств клиентов банков, исключить несанкционированные операции, а также возможность фальсификации, утери и утечки данных клиентов, которые предоставляют последним доступ к финансовым ресурсам [6].

В свою очередь, чтобы использовать собранную биометрию для удаленной идентификации клиентов, ИТ-инфраструктура любого банка должна отвечать серьезным требованиям к обеспечению информационной безопасности защиты данных, предотвращения внешней кибератаки. Вместе с тем комплекс мер по защите биометрических персональных данных достаточно сложный и затратный, и для небольших банков на данный момент недоступен.

В целях дальнейшего развития этой инициативы в банковском секторе крупные банки могут выступить разработчиками безопасного сервисного ландшафта для использования биометрических технологий, создавая полностью готовое решение, и предоставлять его небольшим игрокам, в том числе небанковским организациям как сервис.

Таким образом, в перспективе биометрические технологии расширят возможности практически любого пользователя стать клиентом банка без его посещения, а банкам, их использующим, позволят развить конкурентные преимущества в сфере клиентского обслуживания по сравнению с традиционными банками, имеющими широкую сеть присутствия.

Исследуя вопрос развития и совершенствования биометрических технологий, нельзя не упомянуть мировые тренды в данном направлении.

Согласно данным международного онлайн-провайдера розничных финансовых услуг TCS Group Holding PLC, порядка 70 % всех биометрических технологий в банковском секторе используется в клиентских сервисах, 30 % – в корпоративных целях [12]. При этом в мировой практике уже сейчас успешно применяются такие биометрические технологии как отпечатки пальцев, голос, рисунок вен и геометрия ладони.

При этом основным драйвером роста применения биометрии на мировом финансовом рынке по-прежнему остается активное развитие мобильных технологий и, соответственно, популяризация мобильного банкинга, занимающего уже несколько лет лидирующее положение на цифровом банковском рынке. Современные смартфоны умеют записывать голос, фотографировать изображение лица, а высококачественные камеры и вовсе позволяют идентифицировать человека по радужной оболочке глаза, постепенно становясь мультибиометрическими устройствами [7].

Кроме того, по оценкам международной консалтинговой компании Tech Navio, наиболее перспективными трендами развития биометрических технологий на мировом рынке финансовых услуг являются следующие:

– активное внедрение технологий идентификации клиентов по рисунку вен в ATM и POS-терминалах (технология основана на сканировании узора кровеносных сосудов инфракрасными лучами; признана в мире как один из наиболее высоконадежных способов идентификации);

– широкое использование в работе call-центров технологий голосовой биометрии;

– распространение технологий идентификации по лицу для доступа к мобильным банковским приложениям, при проведении платежей и совершении покупок, а также в ходе процедуры идентификации клиентов в банковских отделениях;

– совершенствование технологий идентификации в мобильном банкинге по отпечаткам пальцев и с использованием систем распознавания по радужной оболочке глаза [12].

Заметим, что немаловажное значение уделяется и вопросам безопасности использования биометрических данных, учитывая, что ежегодно в мирерастет число мошеннических операций и фактов несанкционированного доступа к персональным данным.

Согласно данным международной консалтинговой компании Gartner, мировые расходы на информационную безопасность в 2017 г. достигли 101,5 млрд долл. США, а расходы на кибербезопасность, например, отечественных банков и финансовых организаций составляют порядка 300 млрд рублей в год [9]. В свою очередь, чтобы противостоять киберугрозам, финансовому сектору необходима эффективная система взаимодействия государства и всех участников рынка. О результатах работы последних в данной области необходимо оперативно информировать государственные структуры [8].

Между тем заметим, что регуляторы финансовых рынков различных стран сегодня активно вовлечены в процесс создания высокотехнологичной и безопасной инфраструктуры ДБО. Так, в основе рекомендаций Европейского Центрального банка (далее – ЕЦБ) по обеспечению безопасности проведения платежей лежит принцип многоуровневой аутентификации клиента.

В связи с чем ЕЦБ рекомендует провайдерам услуг ДБО использовать процедуру двух- и более уровневой аутентификации личности клиента, для чего предлагаются на выбор следующие уровни проверки:

– средства логической аутентификации: логин, пароль, идентификационный номер;

– средства физической аутентификации: токены, смарт-карты, мобильные телефоны;

– средства биометрической аутентификации: например, голос, отпечатки пальцев, рисунок радужки глаз и др. [11].

Для российских банков методические рекомендации по нейтрализации угроз безопасности использования биометрии в феврале 2019 г. подготовил Банк России. В частности, Банк России установил правила, позволяющие минимизировать банковские риски при сборе биометрии, обработке запросов физических лиц и их персональных данных, а также непосредственно при проведении удаленной идентификации. В этих целях банкам рекомендовано использовать средства защиты данных современных классов.

Банк России также рекомендует банкам регистрировать все действия операторов, работающих с персональными данными, и информировать их об этом, а также обращает внимание, что для усиления информационной безопасности в ходе сбора биометрии необходимо использовать персональный квалифицированный сертификат ключа проверки электронной подписи.

Сегодня банкам предлагается рассмотреть три варианта организации процесса обеспечения информационной безопасности биометрических данных:

– собственное технологическое решение банка, согласованное с Банком России и ФСБ России;

– типовое технологическое решение, предлагаемое интегратором по информационной безопасности;

– облачное решение поставщика услуг информационной безопасности (в перспективе) [4].

Одновременно отметим, что Банк России, разрабатывая на период 2019-2021 гг. дорожную карту по реализации основных направлений развития финансового рынка Российской Федерации, предусмотрел в ней ряд мероприятий в целях создания благоприятной среды для цифровизации финансового рынка и развития биометрических технологий, в частности оказания содействия развитию конкуренции на финансовом рынке, повышению доступности, качества и ассортимента финансовых услуг, а также снижения рисков в финансовой сфере, к которым относятся следующие:

– повышение уровня информационной безопасности и киберустойчивости, в том числе за счет внедрения в деятельность финансовых организаций национальных стандартов в данной области (плановый срок реализации – 2021 г., при участии ФСБ России и ФСТЭК России);

– развитие платформы для удаленной идентификации, что позволит повысить доступность финансовых услуг, уровень удовлетворенности потребителей финансовых услуг, поспособствует росту конкуренции на финансовом рынке и расширению способов дистанционного получения услуг с помощью ЕСИА и ЕБС (срок реализации – 2021 г., при участии Минкомсвязи России, Росфинмониторинга, Минфина России и ФСБ России);

– обеспечение благоприятных правовых условий для сбора, хранения и обработки биометрии, а именно: снижение регуляторных барьеров для внедрения инновационных бизнес – решений, обеспечение

недискриминационного доступа к данным с дальнейшим усилением фокуса конкуренции в части эффективности обработки данных, а не доступа к ним (срок реализации – 2021 г., при участии Минэкономразвития России, МВД России, ФСБ России, Минкомсвязи России, Роспотребнадзора и ФАС России);

– разработка требований к платформе цифрового профиля с использованием единого технологического идентификатора в целях ускорения и обеспечения легального обмена данными между поставщиками и потребителями финансовых услуг, а также предоставление возможности управлять цифровыми согласиями на обмен данными (срок реализации – 2021 г., при участии Минкомсвязи России);

– создание правового базиса для функционирования и развития платформы «Маркетплейс», что несомненно будет способствовать усилению конкуренции на финансовом рынке, повышению уровня доступности финансовых услуг идальнейшему развитию биометрических технологий (срок реализации – 2020 год, при участии Минфина России и ФАС России) [3; 5].

Учитывая, что сейчас многие банки все еще находятся в стадии разработки проекта и формирования бюджета по подключению к ЕБС и ЕСИА, какие же могут быть приняты банками меры для реализации данного проекта?

Представляется, что план внедрения в банке биометрических технологийможет включать следующие основные мероприятия:

– выбор существующего технологического решения для удаленной идентификации либо разработка нового;

– организация защиты каналов связи между банком и ЕБС;

– интеграция систем банка в тестовый контур ЕБС и ЕСИА, верификация данных и тестирование их передачи;

– отработка процесса получения банковского продукта (услуги) на тестовой группе;

– приобретение и оснащение оборудованием отделений банка, где предполагается проведение биометрической регистрации, настройка соответствующих рабочих мест с последующим направлением документов в Минкомсвязь для оценки их соответствия;

– регистрация идентификационной биометрической системы банка в тестовом контуре межведомственного электронного взаимодействия и получение доступа к тестовым системам ЕБС, ЕСИА;

– внедрение интеграционного решения для сбора биометрических образцов клиентов и системы контроля качества сбора и передачи персональных данных;

– подготовка необходимой внутренней документации и практических инструкций для сотрудников банка, в том числе для Call-центра и техподдержки, обучение сотрудников банка;

– размещение через доступные каналы коммуникации банка адаптированной инструкции Ростелекома по прохождению биометрической регистрации российскими гражданами и информации о предоставлении банком новой услуги своим клиентам [15].

Между тем жизнь вносит свои коррективы. Реалии таковы, что в связи с высокой опасностью распространения короновирусной инфекции (COVID-19) к активному внедрению биометрических технологий сейчас приступили не только банки. Так, в магазинах «Лента» проведено тестирование процедуры покупки товаров с помощью биометрии – такую возможность торговой сети обеспечили ВТБ и Ростелеком, а дальнейшее внедрение биометрического эквайринга для использования в промышленном масштабе планируется уже в середине 2020 г. Переговоры с несколькими крупными розничными сетями по вопросу внедрения оплаты с помощьюбиометрииведет и Промсвязьбанк: пилотные проекты планируется запустить в 2021 г., при этом информация о том, какие именно торговые сети рассматривает банк, пока не раскрывается. Можно также отметить, что в январе 2020 г. пилотный проект по покупке продукциис помощью данных ЕБС был запущен в одной из кофеен Coffee Bean, а в настоящее время проект уже масштабируется на всю торговую сеть. В свою очередь, Ростелеком сообщил, что помимо крупных торговых ритейлеров, внедрение биометрии обсуждается с некоторыми сетями автозаправок и фастфуда, производителями вендинговых автоматов, а также представителями РЖД и московского метрополитена [13].

Таким образом, текущая обстановка может в значительной мере простимулировать развитие биометрических технологий как в России, так и в мире и их дальнейшее внедрение в различные отрасли.

Резюмируя вышесказанное, отметим, что внедрение в России биометрических технологий набирает обороты. Обеспечение данного процесса – большая работа множества государственных структур, которая будет продолжаться и далее, а скорость внедрения биометрических технологий будет напрямую зависеть от поддержки частным бизнесом и населением предлагаемых государством инициатив.

Если удаленная биометрическая идентификация, внедряемая в банковском секторе, а также отдельных крупных торговых ритейлерах при участии банков, продемонстрирует хорошие результаты и не повлечет масштабных проблем, то можно вполне ожидать ее дальнейшего распространения и на другие задачи – государственную безопасность, здравоохранение и иные сферы жизнедеятельности.

На сегодняшний день, одной из ключевых проблем в отношении повсеместного распространения биометрии остается вопрос безопасности как самих баз данных, так и технической инфраструктуры участников проекта. При этом нельзя забывать и об опасениях иного рода: всеобщий сбор биометрических данных при реализации негативных сценариев может послужить ограничению личной свободы и всеобщему контролю над обществомсо стороны государственных структур.

Попутно, отвечая на вопрос, создадут ли в будущем киберпреступники реальную угрозу банковскому сектору, платежной индустрии, государственным структурам и экономике государства в целом, используя потенциальные пробелы в системах биометрической идентификации, можно сказать, что это исключительно вопрос практики.

Библиографический список

1. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 31.12.2017) «О персональных данных» // СПС «КонсультантПлюс» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 29.04.2020).
2. Федеральный закон от 31.12.2017 № 482-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // СПС «КонсультантПлюс» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_286744 (дата обращения: 29.04.2020).
3. План мероприятий («дорожная карта») по реализации Основных направлений развития финансового рынка Российской Федерации на период 2019-2021 годов // Официальный сайт Банка России [Электронный ресурс]. – Режим доступа: https://www.cbr.ru/Content/Document/File/71219/roadmap_onrfr2019_2021.pdf (дата обращения: 29.04.2020).
4. 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 № 4-МР) // СПС «КонсультантПлюс» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_318474/ (дата обращения: 29.04.2020).
5. Ефремов, В. С., Пилишвили, А. С. Перспективы сотрудничества финансовой корпорации и компаний, работающих в сфере цифровых технологий // Управление. – 2019. – № 7 (2). – С. 57-64.
6. Гришина, Е. А. Биометрические технологии в российских банках: мечты или реальность // Наука и общество. – 2015. – № 3 (22). – С. 17-21.
7. Крылова, И. Ю., Рудакова, О. С. Биометрические технологии как механизм обеспечения информационной безопасности в цифровой экономике // Молодой ученый. – 2018. – № 45 [Электронный ресурс]. – Режим доступа: https://moluch.ru/archive/231/53640 (дата обращения: 29.04.2020).
8. Махалин, В. Н., Махалина, О. М. Управление вызовами и угрозами в цифровой экономике России // Управление. – 2018. – № 6 (2). – С. 57-60.
9. Махалина, О. М., Махалин, В. Н. Цифровизация бизнеса увеличивает затраты на информационную безопасность // Управление. – 2020. – № 8 (1). – С. 134-140.
10. Для чего российские банки собирают биометрию, стоит ли ее сдавать и как это сделать // ВсеЗаймыОнлайн [Электронный ресурс]. – Режим доступа: https://vsezaimyonline.ru/reviews/biometrija.html (дата обращения: 29.04.2020).
11. Горшков, А. Использование биометрии для защиты ДБО – новые вехи // Банки.ру [Электронный ресурс]. – Режим доступа: https://www.banki.ru/blog/technoserv/7196.php (дата обращения: 29.04.2020).
12. Обзор международного рынка биометрических технологий и их применение в финансовом секторе // Официальный сайт Банка России [Электронный ресурс]. – Режим доступа: https://www.cbr.ru/Content/Document/File/36012/rev_bio.pdf (дата обращения: 29.04.2020).
13. Опасность распространения коронавируса может стимулировать развитие биометрии // Финмаркет [Электронный ресурс]. – Режим доступа: http://www.finmarket.ru/news/5196963 (дата обращения: 29.04.2020).
14. Официальный сайт Единой биометрической системы [Электронный ресурс]. – Режим доступа: https://bio.rt.ru/citizens (дата обращения: 29.04.2020).

15. План мероприятий (Дорожная карта) банка по реализации проекта подключения к ЕБС // SecurityLab.ru [Электронный ресурс]. – Режим доступа: https://www.securitylab.ru/blog/personal/estekhin/344766.php (дата обращения: 29.04.2020).

References

1. Federal'nyi zakon ot 27.07.2006 № 152-FZ (red. ot 31.12.2017) "O personal'nykh dannykh" [*Federal Law "On Personal Data" No. 152-FZ, dated on July 27, 2006 (as amended, dated on December, 31, 2017)*]. Legal reference system "ConsultantPlus". Available at: http://www.consultant.ru/document/cons_doc_LAW_61801/ (accessed 29.04.2020).
2. Federal'nyi zakon ot 31.12.2017 № 482-FZ "O vnesenii izmenenii v otdel'nye zakonodatel`nye akty Rossiiskoi Federatsii" [*Federal Law "On Amendments to Certain Legislative Acts of the Russian Federation" No. 482-FZ, dated on December 31, 2017*]. Legal reference system "ConsultantPlus". Available at: http://www.consultant.ru/document/cons_doc _LAW_286744/ (accessed 29.04.2020).
3. Plan meropriyatii ("dorozhnaya karta") po realizatsii Osnovnykh napravlenii razvitiya finansovogo rynka Rossiiskoi Federatsii na period 2019–2021 godov [*Action plan ("road map") for the implementation of the Main directions of development of the financial market of the Russian Federation for the period 2019-2021*]. Ofitsial`nyi sait Banka Rossii [*Official website of the Bank of Russia*]. Available at: https://www.cbr.ru/Content/Document/File/71219/roadmap_onrfr2019_ 2021.pdf/ (accessed 29.04.2020).
4. Metodicheskie rekomendatsii Banka Rossii po neitralizatsii bankami ugroz bezopasnosti, aktualnykh pri obrabotke, vklyuchaya sbor i khranenie biometricheskikh personal'nykh dannykh, ikh proverke i peredache informatsii o stepeni ikh sootvetstviya predostavlennym biometricheskim personal'nym dannym grazhdanina Rossiiskoi Federatsii (utv. Bankom Rossii 14.02.2019 № 4-MR) [*Methodological recommendations of the Bank of Russia on the neutralization by banks of security threats relevant to the processing, including the collection and storage of biometric personal data, their verification and the transfer of information on the degree of their compliance with the biometric personal data of the citizen of the Russian Federatio (approved by the Bank of Russia No. 4-MR, dated on February 14, 2019*]. Legal reference system "ConsultantPlus". Available at: http://www.consultant.ru/document/cons_doc_LAW_318474/ (accessed 29.04.2020).
5. Efremov V.S., Pilishvili A.S. Perspektivy sotrudnichestva finansovoi korporatsii i kompanii, rabotayushchikh v sfere tsifrovykh tekhnologii [*Prospects for cooperation between the financial corporation and companies working in the field of digital technologies*]. Upravlenie, 2019, no. 7 (2), pp.57-64.
6. Grishina E.A. Biometricheskie tekhnologii v rossiiskikh bankakh: mechty ili realnost` [*Biometric technologies in Russian banks: dreams or reality*]. Nauka i obshchestvo, 2015, no. 3 (22), pp. 17-21.
7. Krylova I.Yu., Rudakova O.S. Biometricheskie tekhnologii kak mekhanizm obespecheniya informatsionnoi bezopasnosti v tsifrovoi ekonomike[*Biometric technologies as a mechanism for ensuring information security in the digital economy*]. Molodoi uchenyi, 2018, no. 45. Available at: https://moluch.ru/archive/231/53640/ (accessed 29.04.2020).
8. Makhalin V.N., Makhalina O.M. Upravlenie vyzovami i ugrozami v tsifrovoi ekonomike Rossii [*Managing challenges and threats in the Russian digital economy*]. Upravlenie, 2018, no. 6 (2), pp. 57-60.
9. Makhalina O.M., Makhalin V.N. Tsifrovizatsiya biznesa uvelichivaet zatraty na informatsionnuyu bezopasnost' [*Digitalization of business increases the costs on information security*]. Upravlenie, 2020, no. 8 (1), pp. 134-140.
10. Dlya chego rossiiskie banki sobirayut biometriyu, stoit li ee sdavat` i kak eto sdelat` [*Why do Russian banks collect biometrics, is it worth it to take and how to do it*]. VseZaimyOnlain [*VseZaimyOnline*]. Available at: https://vsezaimyonline.ru/reviews/biometrija.html/ (accessed 29.04.2020).
11. Gorshkov A. Ispol`zovanie biometrii dlya zashchity DBO – novye vekhi [*Using biometrics to protect RBS – new milestones*]. Banki.ru. Available at: https://www.banki.ru/blog/technoserv/7196.php/ (accessed 29.04.2020).
12. Obzor mezhdunarodnogo rynka biometricheskikh tekhnologii i ikh primenenie v finansovom sektore [*Review of the international market of biometric technologies and their application in the financial sector*]. Ofitsial`nyi sait Banka Rossii [*Official website of the Bank of Russia*]. Available at: https://www.cbr.ru/Content/Document/File/36012/rev_bio.pdf/ (accessed 29.04.2020).
13. Opasnost' rasprostraneniya koronavirusa mozhet stimulirovat' razvitie biometrii [*The danger of the spread of coronavirus can stimulate the development of biometrics*]. Finmarket. Available at: http://www.finmarket.ru/news/5196963/ (accessed 29.04.2020).
14. Ofitsial`nyi sait Edinoi biometricheskoi sistemy [*Official website of the Unified Biometric System*]. Available at: https://bio.rt.ru/citizens/ (accessed 29.04.2020).
15. Plan meropriyatii (Dorozhnaya karta) banka po realizatsii proekta podklyucheniya k EBS [*The action plan (Road map) of the bank for the implementation of the project connect to the Unified Biometric System*]. SecurityLab.ru. Available at: https://www.securitylab.ru/blog/personal/estekhin/344766.php/ (accessed 29.04.2020).