Государственное и муниципальное управление. Ученые записки. 2022. № 1. С. 89–95
State and Municipal Management. Scholar Notes. 2022;(1):89–95

Проблемы экономики

Научная статья
УДК 336
doi: 10.22394/2079-1690-2022-1-1-89-95

ВОЗМОЖНОСТИ И УГРОЗЫ ЦИФРОВОГО (ОТКРЫТОГО) БАНКИНГА В УСЛОВИЯХ ВНЕДРЕНИЯ API-ИНТЕРФЕЙСА

Софья Сергеевна Дукян[1], Сергей Николаевич Татаркин[2]

[1, 2]Южно-Российский институт управления – филиал Российской академии народного хозяйства и государственной службы при Президенте РФ, Ростов-на-Дону, Россия

[1]duksofia@mail.ru

[2]rgu@inbox.ru

Аннотация. В статье рассматриваются технологии в цифровом банкинге, возможность управления своими финансами, а также сектор финансовых услуг и пути решения для снижения финансовых рисков угрожающих безопасному функционированию банковской системы.

Ключевые слова: банкинг, искусственный интеллект, информационные технологии, финансовые услуги, кредитные карты, API-интерфейс

Для цитирования: Дукян С. С., Татаркин С. Н. Возможности и угрозы цифрового (открытого) банкинга в условиях внедрения API-интерфейса // Государственное и муниципальное управление. Ученые записки. 2022. № 1. С. 89–95. https://doi.org/10.22394/2079-1690-2022-1-1-89-95.

Problems of Economics

Original article

OPPORTUNITIES AND THREATS OF DIGITAL (OPEN) BANKING IN THE CONDITIONS OF IMPLEMENTATION OF THE API INTERFACE

Sof'ya S. Dukyan[1], Sergei N. Tatarkin[2]

[1, 2]South-Russia Institute of Management – branch of Russian Presidential Academy of National Economy and Public Administration, Rostov-on-Don, Russia

[1]duksofia@mail.ru

[2]rgu@inbox.ru

Abstract. The article discusses technologies in digital banking, the ability to manage your finances, as well as the financial services sector and solutions to reduce financial risks that threaten the safe functioning of the banking system.

Keywords: banking, artificial intelligence, information technology, financial services, credit cards, API

For citation: Dukyan S. S., Tatarkin S. N. Opportunities and threats of digital (open) banking in the conditions of implementation of the API interface. *State and Municipal Management. Scholar Notes.* 2022;(1):89–95. (In Russ.). https://doi.org/10.22394/2079-1690-2022-1-1-89-95.

Последние несколько лет финансовый сектор подвержен постоянным изменениям: цифровизация и технологические инновации, изменения потребительских предпочтений, развитие онлайн банкинга. Кризис 2020 г., вызванный пандемией COVID-19, ускорил эти тенденции. Подобные масштабные изменения происходят с человечеством не впервые. В попытках осознать возможности, которые появляются в подобных масштабных изменениях развитие технологий искусственного интеллекта (ИИ) в сфере финансовых услуг, предоставляет банкам потенциал для увеличения доходов при меньших затратах за счет привлечения и обслуживания клиентов радикально новыми способами.

Цифровой банкинг включает в себя множество каналов для предоставления банковских услуг. Такие услуги, как банкоматы, интернет-банкинг, мобильный банкинг, службы приложений, телефонный банкинг и многое другое. По всем этим каналам заказчик может получать необходимые услуги без посредников; поэтому в литературе по цифровому банкингу вводится термин «прямой банкинг» называется [1]. Банковское дело – отныне не место, куда необходимо идти, работать, получать или вкладывать деньги и т.д. Это то, что делаем люди, какие решения и действия они предпринимают. Это банковские продукты и услуги, доступные и представленные клиенту в любое время и в любом месте.

Прямой банкинг позволяет клиентам легко управлять своими финансами, используя онлайн-каналы: подача заявки на получение кредита, открытие нового счета или инвестирование в финансовые рынки, процессы, которые раньше могли занимать часы, дни или даже недели, теперь могут быть выполнены за считанные секунды. Мобильные приложения позволяют пользователям выполнять целый ряд действий всего несколькими кликами в своих смартфонах. Таким образом, общие банковские операции и процедуры ставятся не только более удобными для пользователя, но и доставляют им удовольствие в использовании, формируя лояльность клиента. Помимо этого качество банковского обслуживания определяется уверенностью клиента в предоставляемых в банковской среде услугам [2]. Это связано с тем, что качество и простота предоставления услуг тесно связаны с удовлетворенностью клиентов, поведенческими желаниями и лояльностью клиентов в банковской сфере [3].

Цифровые технологии и их услуги сегодня привлекают внимание многих крупных исследовательских институтов. Сегодня исследуются вопросы влияние технологий с использованием агрегатов больших данных и цифровых кошельков на рост доли рынка [4], исследуется банковский дискурс, описывающий влияние инноваций в области информационно-коммуникационных технологий на банковский и финансовый рынки, влияние банковских каналов, модернизация услуг и снижение затрат с помощью информационных и коммуникационных технологий, рассматривается контекст интернет-банкинга и банковских услуг через призму влияние я ИКТ, рассматриваются вопросы будущего финансовых услуг, изучается настроение клиентов и эффективность бизнеса в финансовой отрасли рассматривает Haraghe Bank в качестве примера).

Традиционно банки неохотно открывали свои данные и системы третьей стороне. Сегодня формируется новая бизнес-модель «умный банк будущего», в центре которой - открытый банкинг, позволяющий третьим лицам получать данные о клиентах от банков (с согласия клиента) и предоставлять ряд новых и инновационных услуг. В результате развивается пользовательский интерфейс в области обслуживания, что неминуемо приведет к возникновению новых угроз безопасности и необходимости создания и предоставления клиентам актуальных безопасных услуг.

Банковская система на протяжении веков придерживалась идеи, что данные, хранящиеся в финансовых учреждениях, изолированы и не могут быть открыты третей стороне. Данный факт означает, что банковская система не может использовать ИИ в полной мере, поскольку последний, обрабатывая большой объем данных, позволяет их использовать для всех видов приложений. И если до 2020 года данный процесс лимитировался, то глобальная пандемия Covid-19 только ускорила переход в цифровую сферу в связи с введенными ограничениями: была остановлена регулярная деятельность банковских отделений, а меры социального дистанцирования еще больше сократили возможность личного взаимодействия. Сложившаяся ситуация спровоцировала стремительный рост использования услуг онлайн и мобильного банкинга практически во всех частях мира, а вместе с ним рост киберпреступлений.

Сектор финансовых услуг стал самой уязвимой отраслью, поскольку основная часть кибератак направлена на банковских клиентов с расширением предоставленных им возможностей принимать финансовые решения с использованием мобильных приложений, а не на учреждения. «Цифровой банкинг, мобильные приложения обеспечивают более быструю обработку финансовых транзакций, что удобней, а так же позволяет продолжать финансовую индустрию даже в условиях пандемии» [5]. Таким образом, встает вопрос об обеспечении безопасности на этапах регистрации, активации или использования мобильного приложения в отношении аккаунта или транзакции, за которыми должна стоять репутация бренда.

Тем не менее, искусственный интеллект может помочь в создании систем, которые значительно быстрее смогут распознавать «мошеннические» транзакции. «Чтобы противостоять кибермошенничеству, банкам необходимо будет выйти за рамки паролей (одноразовых паролей) и активно внедрять биометрические данные, телеметрию устройств и аналитику поведения клиентов».

С этой целью банки должны использовать новые технологии, основанные на современных методах проверки личности для выявления подозрительных транзакций или открытия счетов, что позволит анализировать межканальные данные из нескольких источников, на основе которых в режиме реального времени станет возможным принимать решения в области безопасности, защищать клиентов. Таким образом, крайне важно, чтобы банки обеспечивали клиентам полностью безопасную среду при любых финансовых операциях.

Кража личных данных среди кибермошенничества вызывает наибольшее беспокойство сегодня. «В Российской Федерации, по данным Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России, объем несанкционированных операций со счетов юридических лиц по итогам 2018 г. составил 1,469 млрд руб. (в 2017 г. - порядка 1,57 млрд руб., в 2016 г. - порядка 1,89 млрд руб., в 2015 г. - порядка 3,7 млрд руб.).

На территории России и за ее пределами объем несанкционированных операций с использованием платежных карт, эмитированных российскими кредитными организациями, в 2018 г. составил 1,384 млрд руб. (в 2017 г. – 0,961 млрд руб., в 2016 г. – 1,08 млрд руб., в 2015 г. – 1,14 млрд руб.).

Удельный вес таких операций в общем объеме операций с использованием платежных карт, эмитированных российскими кредитными организациями, в 2018 г. составил 0,0018% (1,8 копейки на 1000 рублей переводов).

Существуют определенные лимиты, несанкционированных переводов денежных средств, установленные Европейской службой банковского надзора (EBA), которые составляют 0,005% (5 евроцентов на 1000 евро переводов)[1].

Более наглядно ситуация 2019 – 2020 гг. представлена на рис. 1.

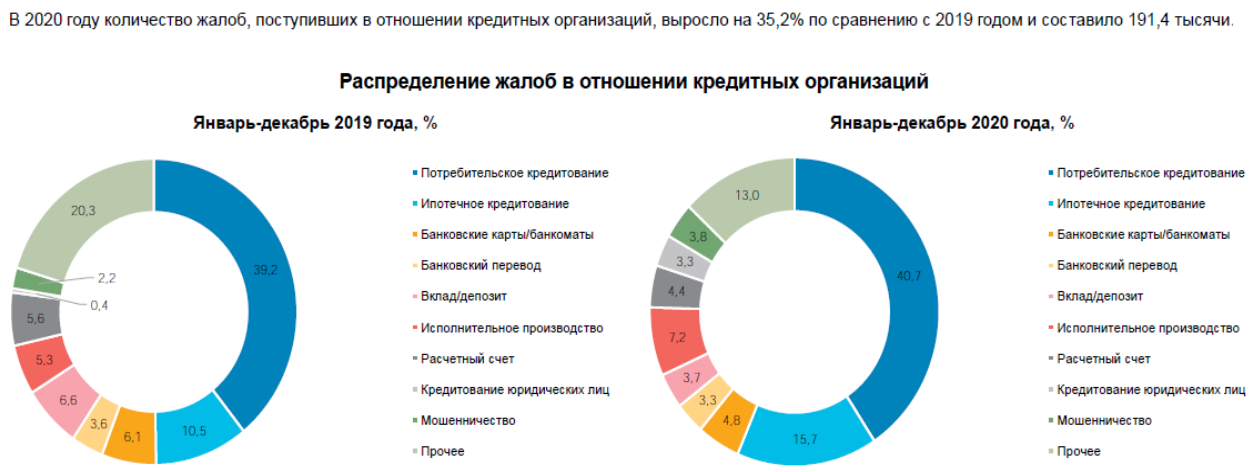

Рис. 1[2]. Распределение жалоб в отношении организаций

Fig. 1. Distribution of complaints against organizations

Мошенничество с кредитными картами, кража личных данных является одной из самых распространенной жалоб. Этому способствует растущая с каждым днем онлайн-торговля, покупка товаров через Интернет и т.д. В случае, взлома хакерами цифровой инфраструктуры банка, кража личных данных становится серьезным риском для клиентов, который невозможно игнорировать (в последнее время кража учетных записей стала особенно популярной): третья сторона, мошенники, получают доступ к учетной записи пользователя, с помощью которой преступник может изменить данные учетной записи, выдавая себя за пользователя. Поскольку все последующие обновления учетной записи перенаправляются на контактный адрес преступника, пользователь часто ничего не знает о произведенной кибератаке.

[1] https://www.garant.ru/products/ipo/prime/doc/74615166/
[2] https://cbr.ru/Collection/Collection/File/31975/2020_4.pdf

Распространение вирусного программного обеспечения также является серьезной и растущей проблемой. Часто это принимает форму автоматических угроз, таких как программы-вымогатели, которые должны выглядеть как обычные, законные электронные письма от известных корреспондентов. На самом деле, однако, это фишинговые электронные письма, которые предлагают пользователю загрузить небезопасное вложение, содержащее программу-вымогатель, которая может заблокировать доступ пользователя к его учетной записи, а затем злоумышленник требует выплаты в обмен на снятие блокировки.

Ежегодно наблюдается значительное увеличение числа «скомпрометированных» кредитных карт, утечек учетных данных и вредоносных приложений. Финансовые преступления представляет собой махинацию цифр: чем больше украденных номеров учетных записей, к которым может быть получен доступ, или запущенных фишинговых сайтов, тем больше у мошенников шансов на успех. Во всем мире банки сталкиваются с более частыми и агрессивными кибератаками, и серьезность и изощренность этих атак постоянно возрастают. Времена, когда простой текстовый пароль в сочетании с запоминающимся словом или девичьей фамилией матери пользователя считался достаточно надежной защитой, давно прошли. Общество же все больше стремится к простому обслуживанию с помощью финансовых технологий. Самым разумным для финансовых учреждений становится интеграция новых услуг от новых партнеров, осуществляющееся через венчурные компании и реальные финансовые ускорители, каждый из которых, в свою очередь, имеет общую стратегию цифровой трансформации.

Тем не менее, финансовая отрасль больше осознает появляющиеся риски, угрожающие безопасному функционированию цифровых банковских услуг, и принимает все возможные меры для их снижения. На сегодняшний день реальным решением проблемы стала интеграция подхода API платформы для управления и обеспечения безопасности финансовых операций. Открытые технологии API позволяют разработчикам сторонних программ использовать стандарты безопасности, установленные банком. Аутентификация с помощью банковской учетной записи гарантирует безопасность проводимых финансовых операции в сторонних приложениях, исключает утечку персональных данных, которые могут использовать мошенники.

Интеграция API-платформ в финансовые операции позволяет обеспечить клиентов гибкими услугами за счет сторонних поставщиков данных услуг, расширения спектра услуг и финансовых продуктов, то есть все ключевые аспекты цифрового банка. С внедрением API цифровой банкинг получает новую архитектуру, в которой API становится соединительной тканью, обеспечивающей контролируемый доступ к услугам, продуктам и данным как внутри банка, так и за его пределами. Внутри банка API-интерфейсы сокращают потребность в разных хранилищах, увеличивают возможность повторного использования технологических активов и способствуют гибкости цифрового банкинга.

Помимо банка, API-интерфейсы ускоряют возможности внешнего партнерства, открывают новые возможности для бизнеса и улучшают качество обслуживания клиентов. Хотя API-интерфейсы могут принести значительную пользу, очень важно начать с определения того, где они будут использоваться [6]. Следовательно, API содействуют повторному использованию и ускорять работу, обеспечивая доступ к детализированным сервисам (внутренним и внешним), упрощает и ускоряет сотрудничество с внешними партнерами, повышает качество обслуживания клиентов, предоставляя своевременный доступ к данным и сервисам (для разных команд) и т.д.

Банки должны интегрировать внутренние и внешние системы для поддержки беспрепятственного взаимодействия клиентов с внутренними платформами, партнерскими экосистемами и многочисленными внешними интерфейсами, что в свою очередь, требует надежного и стандартизированного подхода для внедрения API. Когда определен набор API-интерфейсов, координирующих потоки между системами, появляется возможность продвигать инновации от концепции к жизнеспособному продукту за 30–60 дней. При этом надежность и бесперебойность интеграции API зависит от высокоскоростного канала потоковой передачи данных, и стандартизованной асинхронной передачи данных в режиме реального времени. Использование современной облачной инфраструктуры для размещения платформ также упрощает масштабирование.

Такой шаг дает возможность разработать стандарты, позволяющие банкам взять на себя большую ответственность за безопасность данных клиентов и функционировать эффективно, например перевод основного банковского обслуживания в облако с общим доступом.

Центробанк России уже объявил о готовности стандартов открытых банковских интерфейсов (API), разработанных совместно с участниками российского финансового рынка на площадке

Ассоциации развития финансовых технологий «Финтех» (АФТ). Предполагается, что внедрение новых стандартов на данном этапе будет добровольным[1].

Апробацию уже прошли «Точка» и Промсвязьбанк. Еще ряд финансовых организаций находятся на этапе подключения. Первой услугой с использованием открытых API станет возможность обмена информацией по счетам юридических лиц между банками. Благодаря этому при оформлении кредита компаниям не нужно будет предоставлять в банк-кредитор бумажные выписки по счетам из других банков; достаточно дать согласие на передачу этих сведений в электронном виде банку-кредитору. При этом участники используют единые стандарты открытых API и присоединяются к единым правилам, без необходимости заключения дополнительных договоров друг с другом[2].

Еще одним из нововведений является, то что с 1 октября 2021 г. платежи по QR-коду станут обязательными для системно значимых банков. Их 12, к ним относятся «Сбербанк», ВТБ, «Газпромбанк», «Альфа-банк», «Райффайзенбанк», «Юникредит», «Совкомбанк», «Московский кредитный банк», «Открытие», «Росбанк», «Промсвязьбанк» и «Россельхозбанк».

Банки с универсальной лицензией должны обеспечить оплату по QR-коду в СБП с 1 апреля 2022 года. Изменения в Положение «О платежной системе Банка России» зарегистрировал Минюст.

К этому периоду кредитные организации также обязаны будут настроить проведение других типов операций СБП: переводов между гражданами по инициативе получателя, а также платежей от юридического лица физическому.

Системно значимые банки также обязали предоставить клиентам возможность совершать расчеты по QR-кодам через СБП с помощью мобильных приложений. Для физлиц – с 1 апреля 2021 г., а для юридических лиц – с 1 апреля 2022 г. Разработкой приложения для оплаты покупок занимается Национальная система платежных карт.

Возможность расчетов по QR-кодам через СБП Центробанк запустил в начале 2019 года. С помощью системы клиенты могут переводить друг другу деньги по номеру телефона, а также оплачивать товары и услуги посредством QR-кода[3].

В условиях создания и внедрения новейших технологий и услуг банки должны обеспечить своевременное и актуальное обучение своих сотрудников с целью своевременного выявления потенциальных рисков и обеспечения безопасности, готовых моментально реагировать в чрезвычайных ситуациях, складывающихся по различным сценариям нарушения безопасности. В отношении клиентов банки обязаны разработать соответствующие действующие процедуры и информировать их о таких возможностях или алгоритме действий.

Сегодня в распоряжении клиентов есть целый ряд возможностей для усиления защиты от киберпреступников. Например, многофакторная аутентификация, которая уже доказала свою высокую эффективность: в дополнение к обычному текстовому паролю требуется, по крайней мере, одна дополнительная форма проверки личности, прежде чем клиент сможет получить доступ к своему счету в цифровом банке. Некоторые из наиболее популярных форм проверки включают одноразовые пароли для входа в систему, действующие в короткий временной промежуток. Подобные пароли обычно включают коды, отправляемые через SMS или приложения-аутентификаторы. Поскольку хакер вряд ли также будет владеть мобильным телефоном пользователя, данный метод значительно снижает вероятность взлома учетной записи. Другие распространенные формы дополнительной проверки личности, как правило, включают биометрию: для проверки личности пользователя используется аутентификация по отпечаткам пальцев или распознаванию лица.

Дополнительной эффективной мерой, направленной на защиту клиента, становится определение сценария, по которому он с большей степенью вероятности может стать мишенью фишинговых мошенников (не пользоваться общедоступными сетями Wi-Fi при доступе к своим учетным записям в цифровом банке, периодически обновлять пароли, использовать и различные пароли для разных банковских приложений).

Хотя угрозы кибербезопасности, возникающие с использованием ИИ, открытого банкинга и т.д. увеличивают риск мошенничества, банкам потребуется применять новые и более сложные меры для предотвращения подобных случаев и повышения безопасности в финансовом секторе. Ключом решения проблем станет, как не парадоксально, более широкое внедрение технологий ИИ, которые помогут банкам быстрее обнаруживать аномалии и, возможно, в один прекрасный день полностью остановить их возникновение. Таким образом, с учетом смены парадигмы финансовых

[1] https://www.cnews.ru/news/top/2020-10-26_tsentrobank_rossii_standartiziroval
[2] https://smebanking.news/ru/39263-razvitie-otkrytyx-api-v-bankax-rossii/
[3] https://rb.ru/news/banki-qr-kod/

услуг от традиционного банкинга к цифровому, определяются следующие факторы качества современных банковских услуг:

• В области персонализации информации и услуг: 1) персонализация пользовательского интерфейса с учетом предпочтений; 2) получение консультационных и плановых услуг; 3) получение информации о клиенте; 4) получение исчерпывающей информации в личном кабинете клиента; 5) получение обновленной информации; 6) предоставление услуг по платежам; 7) предоставление интерактивных услуг через робот-чаты; 8) обеспечение возможности повторяющихся задач с планированием; 9) возможность определения и предложения услуг P2P; 10) предоставление информации клиентам; 11) управление рисками; 12) помощь в принятии решений на основе моделирования; 13) консультирование клиентов по вопросам инвестирования; 14) предоставление информации о покупательной способности покупателя после каждой его операции и т.д.

• В области безопасности и аутентификации: 1) интегрированная аутентификация во всех банковских каналах; 2) биометрическая аутентификация через мобильный телефон и другие устройства, например киоск; 3) наличие достаточного количества индикаторов безопасности; 4) предотвращение несанкционированного доступа; 5) сохранение информации и конфиденциальности пользователя; 6) выход из учетных записей пользователей при отключении от Интернета или продлении транзакции; 7) изменение секретных вопросов; 8) учетная запись пользователя активна во время выполнения транзакции; 9) управление «ненормальными» транзакциями; 10) восстановление пароля; 11) выявление и расследование мошенничества; 12) обеспечение конфиденциальности для клиентов; 13) включение аутентификации с помощью различных методов, таких как отпечаток пальца, глаз и так далее; 14) определение уровня доступа в юридическом банке; 15) наличие ошибки при обработке транзакции.

• В области сервисных инноваций: 1) открытый API (открытый банкинг); 2) управление заработной платой с открытым API; 3) ведение бухгалтерского учета с открытым API; 4) автоматическая проверка клиентов; 5) автоматическое обучение и постоянное совершенствование в предоставлении клиентам различных и конкретных услуг; 6) предоставление услуг краудфандинга; 7) предоставление услуг на носимых устройствах; 8) предоставление услуг с оборудованием IoT; 9) обеспечение прогнозируемой модели бизнеса; 10) предоставление прикладных программ в различных приложениях; 11) предоставление услуг виртуальных филиалов; 12) предоставление услуг в социальных сетях; 13) с использованием технологии блокчейн; 14) обмен на иностранную и внутреннюю цифровую валюту (возможность свопа); 15) с использованием криптовалют; 16) возможность инвестирования в проекты финансирования; 17) предоставление онлайн-услуг, таких как открытие онлайн-счета, сбережения и т. д.; 18) автоматическая классификация клиентов для выдачи кредита; 19) предоставление роботизированных услуг, таких как робот-говорящий, в банковских каналах; 20) анализ поведения клиентов; 21) предлагая интегрированные услуги по всем каналам.

Список источников

1. Arner, D. W., Barberis, J., & Buckley, R. P. (2015). The evolution of Fintech: A new post-crisis paradigm. Geo. J. Int'l L., 47, 1271.

2. Lee, I., & Shin, Y. J .(2018). Fintech: Ecosystem, business models, investment decisions, and challenges. Business horizons, 61(1), 35-46.

3. Omarini, A. (2017). The digital transformation in banking and the role of FinTechs in the new financial intermediation scenario. /
https://www.researchgate.net/publication/319464893_The_Digital_Transformation_in_Banking_and_The_Role_of_FinTechs_in_the_New_Financial_Intermediation_Scenario

4. Patel, I. H., & Bhatt, V. (2018). Development of Model to Evaluate Service Quality Gap in the Generation of Digital Banking /
https://www.researchgate.net/publication/335600926_Development_of_Model_to_Evaluate_Service_Quality_Gap_in_the_Generation_of_Digital_Banking

5. Barberis, J., Chist, Susanne. (2016). The FINTECH Book: The Financial Technology Handbook for Investors, Entrepreneurs, and Visionaries /
https://www.researchgate.net/publication/318790084_THE_FINTECH_BOOK_THE_FINANCIAL_TECHNOLOGY_HANDBOOK_FOR_INVESTORS_ENTREPRENEURS_AND_VISIONARIES

6. Renny Thomas, Vinayak HV, Raphael Bick, and Shwaitang Singh (2019) Ten lessons for building a winning retail and small-business digital lending franchise //
https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/ten-lessons-for-building-a-winning-retail-and-small-business-digital-lending-franchise

References

1. Arner, D. W., Barberis, J., & Buckley, R. P. (2015). *The evolution of Fintech: A new post-crisis paradigm.* Geo. J. Int'l L., 47, 1271.

2. Lee, I., & Shin, Y. J. (2018). Fintech: Ecosystem, business models, investment decisions, and challenges. *Business horizons*, 61(1), 35-46.

3. Omarini, A. (2017). The digital transformation in banking and the role of FinTechs in the new financial intermediation scenario. Available from: https://www.researchgate.net/publication/319464893_The_Digital_Transformation_in_Banking_and_The_Role_of_FinTechs_in_the_New_Financial_Intermediation_Scenario

4. Patel, I. H., & Bhatt, V. (2018). Development of Model to Evaluate Service Quality Gap in the Generation of Digital Banking. Available from: https://www.researchgate.net/publication/335600926_Development_of_Model_to_Evaluate_Service_Quality_Gap_in_the_Generation_of_Digital_Banking

5. Barberis, J., Chist, Susanne. (2016). The FINTECH Book: The Financial Technology Handbook for Investors, Entrepreneurs, and Visionaries. Available from: https://www.researchgate.net/publication/318790084_THE_FINTECH_BOOK_THE_FINANCIAL_TECHNOLOGY_HANDBOOK_FOR_INVESTORS_ENTREPRENEURS_AND_VISIONARIES

6. Renny Thomas, Vinayak HV, Raphael Bick, and Shwaitang Singh (2019). Ten lessons for building a winning retail and small-business digital lending franchise. Available from: https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/ten-lessons-for-building-a-winning-retail-and-small-business-digital-lending-franchise

Информация об авторах

С. С. Дукян – канд. филос. наук, доц. кафедры экономики, финансов и природопользования;

С. Н. Татаркин – канд. экон. наук, доц. кафедры экономики, финансов и природопользования.

Information about the authors

S. S. Dukyan – Candidate of Philosophical Sciences, Associate Professor of the Department of Economics, Finance and Environmental Management;

S. N. Tatarkin – Candidate of Economic Sciences, Associate Professor of the Department of Economics, Finance and Environmental Management.

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации.
Авторы заявляют об отсутствии конфликта интересов.

Contribution of the authors: the authors contributed equally to this article. The authors declare no conflicts of interests.

Статья поступила в редакцию 17.01.2022; одобрена после рецензирования 04.02.2022; принята к публикации 05.02.2022.
The article was submitted 17.01.2022; approved after reviewing 04.02.2022; accepted for publication 05.02.2022.