УДК 336.71(045)

Цифровое взаимодействие с клиентом в процессе заключения договора финансовой организацией

Емец Михаил Игоревич,
студент магистратуры факультета анализа рисков и экономической безопасности, Финансовый университет,
Москва, Россия
memets@ya.ru

Аннотация. *Цель статьи — с прикладной точки зрения рассмотреть современные подходы к дистанционному взаимодействию с клиентом, оценить возможности финансовых организаций в Российской Федерации для дистанционного заключения договора с клиентом. Развитие информационных технологий на сегодняшний день позволяет осуществлять взаимодействие субъектов экономических отношений дистанционно, в том числе — при оказании финансовых услуг, что подтверждается статистикой проникновения Интернета в России. Обзор западных источников позволяет сформулировать причины, обуславливающие важность дистанционного взаимодействия с клиентом, а также преимущества заключения договора в цифровом формате. Описываются возможности для дистанционного взаимодействия с клиентом финансовой организации, созданные в Российской Федерации с учетом международных требований к противодействию отмыванию доходов и финансированию терроризма (ПОД/ФТ). Методологическую обоснованность исследованию обеспечивает применение научных методов: анализа и синтеза, аналогии, сравнения. Основным результатом можно считать рассмотрение сущности Единой биометрической системы, имеющей потенциал платформы дистанционной биометрической идентификации, важной в контексте построения цифровой экономики в Российской Федерации. Таким образом, на сегодняшний день создана инфраструктура для дистанционного заключения договора (в том числе договора банковского счета) с соблюдением международных стандартов по надлежащей проверке клиентов, однако на первоначальном этапе только 4 банка готовы предлагать клиентам услуги по дистанционному открытию счетов. Требуется время для адаптации банков к новым требованиям по информационной безопасности в связи с работой Единой биометрической системы.*

Ключевые слова: *дистанционное заключение договора; удаленная идентификация; биометрия; ПОД/ФТ; Единая биометрическая система (ЕБС); Единая система идентификации и аутентификации (ЕСИА)*

Digital Interaction with the Client in the Process of Concluding a Contract by a Financial Institution

Emets Mikhail Igorevich,
Master's student, Faculty of Risk Analysis and Economic Security, Financial University, Moscow, Russia
memets@ya.ru

Научный руководитель: ***Дадалко В.А.,*** *доктор экономических наук, профессор кафедры анализа рисков и экономической безопасности, Финансовый университет, Москва, Россия.*

Abstract. *The purposes of the article are to consider modern approaches to remote interaction with the client and to define the possibilities of financial institutions in the Russian Federation for the remote signing of the contract with clients. The development of information technologies today allows for the interaction of subjects of economic relations remotely, including — in the provision of financial services, as evidenced by the statistics of Internet penetration in Russia. The review of sources allows formulating the reasons for the importance of remote interaction with clients, as well as the advantages of signing a contract in digital format. The article describes the opportunities for remote interaction with clients of a financial organisation following international requirements for combating money laundering and financing of terrorism (AML/CFT). Methodological validity of the study provides the use of scientific methods, such as analysis and synthesis, analogy, comparison. The main result is defining the essence of the Unified biometric system with the potential of a remote biometric identification platform, which is vital in the context of building the digital economy in the Russian Federation, is considered. Today the infrastructure for the remote signing of the contract (including the bank account) in compliance with international standards for the customer due diligence, but today only four banks are ready to offer customers services for remote account opening. It takes time for banks to adapt to the new requirements for information security in connection with the operation of the Unified biometric system.*

Keywords: *remote contract signing; remote identification; biometrics; AML/FT; unified biometric system; unified identification and authentication system; ESIA*

Введение

На сегодняшний день информационные технологии развиты настолько, что позволяют осуществлять почти все виды взаимодействия дистанционно, без личного присутствия. Интернет-коммерция, онлайн-образование, дистанционные судебные процессы, государственные услуги, телемедицина — эти и другие направления активно развиваются в последние годы. Способствует этим процессам проникновение Интернета, в том числе с помощью распространения смартфонов. По данным исследования[1], проникновение Интернета в России в 2019 г. превысило 75%. При этом 35% всех пользователей Интернета в России пользуются доступом в Сеть только с мобильных устройств.

Финансовый сектор, в том числе банки, традиционно характеризуется широким применением инноваций, возник и специальный термин «финтех», описывающий связь финансов и технологий. Технически договор с клиентом может быть заключен дистанционно (подписание электронной подписью), последующее обслуживание также производится дистанционно. Для описания процесса заключения договора в электронном виде в английском языке существует специальный термин — "digital onboarding"[2], для которого затруднительно подобрать полноценный перевод на русский язык. По смыслу "digital onboarding" означает цифровое (дистанционное) взаимодействие с клиентом, заключение договора в электронном виде. Целью исследования является рассмотрение с прикладной точки зрения современных подходов к дистанционному взаимодействию с клиентом, оценка возможностей финансовых организаций в Российской Федерации для дистанционного заключения договора с клиентом.

Методы исследования

Исследование основано на анализе западных источников, в том числе исследований консалтинговых компаний, посвященных дистанционному взаимодействию с клиентом в процессе заключения договора (от англ. digital onboarding). Проведен анализ динамики российского законодательства, в которое последовательно было внедрено сначала понятие упрощенной идентификации клиента — физического лица для заключения отдельных видов договоров при условии, что все расчеты проводятся в безналичном порядке по счетам, открытым в российских кредитных организациях; далее созданы возможности и для дистанционного открытия банковских счетов с использованием Единой биометрической системы. Проанализированы рекомендации Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ), их внедрение в российскую практику.

[1] Исследование GfK: Проникновение Интернета в России. URL: https://www.gfk.com/ru/insaity/press-release/issledovanie-gfk-proniknovenie-interneta-v-rossii-1/ (дата обращения: 10.04.2019).

[2] Digital Onboarding. URL: https://www.moneyland.ch/en/digital-onboarding-definition (дата обращения: 10.04.2019).

Результаты исследования

В докладе консалтинговой компании Deloitte[3] приводятся 3 причины, обуславливающие важность цифрового взаимодействия с клиентом:

1. Снижение соотношения затраты/доход: для традиционных финансовых институтов в Европе это становится вызовом, особенно в свете развития небольших финтех-компаний и роста регуляторной нагрузки. Заключение договора с клиентом в электронном виде позволяет снизить издержки и улучшить соотношение затраты/доход.

2. Поведение клиентов развивается в сторону использования цифровых технологий: клиенты ожидают возможности получать любые услуги, в любом месте и в любое время. По статистике компании Deloitte, до 38% потенциальных клиентов могут отказаться от заключения договора из-за необходимости подписания бумажных документов и количества запрашиваемой информации.

3. Новые участники рынка изменяют ландшафт рынка предоставления финансовых услуг. С одной стороны, финтех-компании предоставляют удобный сервис для клиентов и повышают конкуренцию между традиционными финансовыми компаниями, с другой стороны, новые технологии позволяют традиционным финансовым компаниям изменяться и соответствовать новым ожиданиям клиентов.

В указанном исследовании Deloitte также называются преимущества цифрового взаимодействия с клиентом, заключения договора в электронном виде:

- более быстрый и гибкий доступ к финансовым услугам;
- поддержание образа инновационной компании;
- возможность перемещать обслуживание из физических офисов в дистанционный формат;
- возможность заключать договоры значительно быстрее;
- повышение структурированности файлового архива, минимизация потерь документов и снижение использования бумаги;
- понижение стоимости обслуживания клиентов;
- повышение эффективности продаж;
- высвобождение времени сотрудников и т.д.

Финансовые организации в процессе заключения договора с клиентом должны соблюдать определенные регуляторные требования, в том числе — требования, связанные с противодействием отмыванию доходов и финансированию терроризма (ПОД/ФТ). На международном уровне подходы ПОД/ФТ разрабатывает межправительственная организация — Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ). Основным методическим источником ФАТФ по ПОД/ФТ являются 40 рекомендаций[4]. Государства, в целях соответствия указанным требованиям, должны на национальном уровне внедрить и детализировать эти рекомендации. В частности, 10-я рекомендация ФАТФ «Надлежащая проверка клиентов» требует, чтобы финансовые организации не открывали анонимные счета, а также счета, открытые на вымышленные имена. Эта рекомендация требует, в том числе, проведения идентификации и установления личности клиента с использованием надежных, независимых первичных документов, данных или информации. В российское законодательство рекомендации ФАТФ внедрены через принятие специального закона — «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»[5].

В 2014 г. в указанный федеральный закон введено понятие «упрощенная идентификация клиента — физического лица» [1]. Упрощенная идентификация предусматривает сбор ограниченного набора сведений в отношении клиента и может проводиться дистанционно, что прямо предусматривают два из трех способов упрощенной идентификации. В соответствии с п. 1.12 ст. 7 № 115-ФЗ, упрощенная идентификация клиента — физического лица проводится одним из следующих способов:

1) личное предоставление клиентом — физическим лицом документов;

2) направление клиентом — физическим лицом финансовой организации предусмотренных иден-

[3] Digital onboarding for financial services. A must-have for digital natives. URL: https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/technology/lu-digital-onboarding-financial-services-digital-natives-112017.pdf (дата обращения: 11.04.2019).

[4] Рекомендации ФАТФ. Международные стандарты по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения. Пер. с англ. М.: Вече; 2012. 176 с.

[5] Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (ред. от 18.03.2019). Доступ из справ.-правовой системы «Консультант-плюс».

тификационных сведений о себе, а также СНИЛС, и/или ИНН, и/или номера полиса ОМС, а также номера мобильного телефона;

3) авторизация клиентом — физическим лицом в ЕСИА с подтвержденной учетной записью, указание предусмотренных идентификационных сведений и СНИЛС.

Федеральным законом закреплено, что проводиться упрощенная (в том числе дистанционная) идентификация может только при заключении определенных договоров и только при условии, что все расчеты будут осуществляться исключительно в безналичной форме по счетам, открытым в российской кредитной организации:

- договор потребительского кредита (займа) с учетом установленных особенностей;
- договор с негосударственным пенсионным фондом;
- договор о брокерском/депозитарном обслуживании;
- договор доверительного управления ценными бумагами;
- при приобретении инвестиционных паев паевых инвестиционных фондов.

По логике законодателя, проведение расчетов в безналичной форме по счетам, открытым в российском банке, снижает риск вовлечения в ОД/ФТ и прочие сопутствующие риски, так как для открытия банковского счета клиент должен обратиться лично. Абзац 3 п. 5 ст. 7 Федерального закона № 115-ФЗ запрещает банкам открывать банковские счета без личного присутствия клиента (представителя клиента). Однако в 2018 г. вступил в силу федеральный закон[6], вводящий исключение из этого правила. Нормами данного закона в Российской Федерации создается Единая биометрическая система (ЕБС), а также закрепляется возможность применять биометрические технологии для идентификации граждан.

Дистанционная аутентификация (подтверждение подлинности) — самый распространенный метод дистанционного подтверждения личности [2]. Существуют три фактора аутентификации:

1) то, что пользователь знает: например, пароль;

2) то, что пользователь имеет: например, физический носитель (токен);

3) то, чем пользователь является: например, биометрические параметры: изображение, голос, радужка глаза и т.д.

Простейшие механизмы аутентификации построены только на паролях (то, что пользователь знает). Основная проблема этого метода — низкая надежность, так как пароли можно подобрать, особенно если пользователь использует простое сочетание символов. Более надежный механизм — комбинация пароля и физического носителя (токена), что в совокупности представляет собой двухфакторную аутентификацию. Однако и такая двухфакторная аутентификация не является вполне надежной, так как оба фактора могут быть скомпрометированы одновременно: например, если злоумышленник получил доступ и к паролю, и к физическому носителю. Следующий уровень надежности — то, чем пользователь является, например биометрические параметры. Этот фактор аутентификации не может быть легко потерян или забыт, но в этом заключается и его недостаток: скомпрометированные биометрические параметры человека нельзя заменить, что порождает строгие требования к обработке и хранению биометрии. В модели российской Единой биометрической системы используется комбинация двух факторов: логин/пароль от учетной записи в ЕСИА (то, что пользователь знает) и биометрические характеристики, хранящиеся в ЕБС (то, чем пользователь является).

На текущий момент размещать биометрические персональные данные в ЕБС вправе только уполномоченные банки, для государственных органов и иных организаций такие возможности не созданы. Использовать биометрические данные в целях идентификации допускается для дистанционного открытия банковских счетов.

Работает данный механизм следующим образом. Гражданин при личном обращении в уполномоченный банк регистрируется в Единой биометрической системе (применяются две модальности: изображение лица и запись голоса) и в Единой системе идентификации и аутентификации — ЕСИА (если ранее не было подтвержденной учетной записи на портале Госуслуг). В дальнейшем у этого гражданина появляется возможность проходить дистанционную идентификацию с помощью компьютера или смартфона для открытия банковских счетов в тех банках, в которых он не является клиентом без необходимости личного обращения, подписания бумажных документов (при условии, что такой банк

[6] Федеральный закон от 31.12.2017 № 482-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации». Доступ из справ.-правовой системы «Консультант-плюс».

предоставляет услугу дистанционного открытия банковских счетов с применением ЕБС). Итак, ЕБС потенциально представляет собой платформу для дистанционной биометрической идентификации.

В чем специфика платформы для дистанционной идентификации в отличие от традиционной схемы идентификации клиента? В традиционной схеме каждая финансовая организация собирает в отношении клиента одинаковый набор идентификационных сведений, предусмотренных в нормативных актах. Как следствие — потенциальному клиенту для каждой финансовой организации, с которой он планирует заключить договор, необходимо предоставить одинаковый набор сведений. В случае платформы для идентификации идентификационные сведения в отношении каждого лица размещаются в единой базе данных (см. *рисунок*). В процессе первичной идентификации или планового обновления сведений финансовая организация будет обращаться для сбора этих сведений не к самому клиенту, а к базе данных идентификационной платформы. Концепция такого механизма идентификации была описана, в частности, в докладе консалтинговой компании PWC в 2015 г.[7]

Преимущества платформы перед классической моделью очевидны: экономия на масштабе за счет устранения дублирования процедур, ускорение принятия новых клиентов, унификация подходов к идентификационным процедурам в различных организациях.

По состоянию на апрель 2019 г., т.е. спустя 10 месяцев после вступления в силу указанных изменений, только 4 банка предоставляют услугу дистанционного открытия счетов с применением биометрических технологий: ПАО «Почта Банк», АО «Тинькофф банк», ПАО «Совкомбанк», ООО «Хоум Кредит энд Финанс Банк»[8].

В чем причины относительно невысокой распространенности услуг с применением биометрических технологий среди банков?

Во-первых, подготовка подключения к Единой биометрической системе требует значительных инвестиций. По оценке экспертов, минимальные затраты для подключения банка с одним отделением составляют 4 млн руб., далее дополнительно 130 тыс. руб. за каждое отделение[9]. Очевидно, не следует ожидать от этих вложений моментальной отдачи, так как потенциальный приток клиентов, полученных по дистанционному каналу, может окупиться только при более длительной истории обслуживания.

Во-вторых, учитывая необходимость сохранения конфиденциальности биометрических данных, существуют жесткие нормативные требования по информационной безопасности и техническому соответствию при обработке биометрических персональных данных[10]. Соответствие этим требованиям может быть вызовом для небольших банков, не всегда имеющих в штате специалистов по информационной безопасности соответствующего уровня. Передача этих работ на аутсорсинг также потребует финансовых вложений. Необходимость соответствия этим требованиям обусловлена чувствительностью биометрических данных к потере конфиденциальности: как отмечалось выше, в случае компрометации, человек не сможет «заменить» свои биометрические характеристики по аналогии с паролем. Специалисты выделяют следующие риски, связанные с безопасностью биометрических данных:

- кража биометрической информации с сервиса авторизации;
- перехват биометрической информации, передаваемой по сети;
- чтение биометрической информации со взломанного устройства;
- кража биометрической информации «с человека» или с носителя информации [3].

В-третьих, дистанционная идентификация актуализирует риски, связанные с поддельными документами. Складывается ситуация, в которой банки — участники Единой биометрической системы вынуждены полагаться на качество проверки документов, проведенной сотрудником уполномоченного банка, регистрировавшего клиента впервые. Для минимизации этого риска сотрудники уполномоченных банков должны иметь знания по выявлению

[7] Share and share alike: meeting compliance needs together with a KYC utility. URL: https://www.pwchk.com/en/financial-services/fs-kyc-utlilty-dec2015.pdf (дата обращения: 13.04.2019).

[8] Единая биометрическая система | Гражданам. URL: https://bio.rt.ru/citizens/ (дата обращения: 13.04.2019).

[9] Банки оценили биометрию. Газета «Коммерсант». URL: https://www.kommersant.ru/doc/3731093 (дата обращения: 13.04.2019).

[10] Приказ Минкомсвязи России от 25.06.2018 № 321 «Об утверждении порядка обработки...». Доступ из справ.-правовой системы «Консультант-плюс»; приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных...». Доступ из справ.-правовой системы «Консультант-плюс».

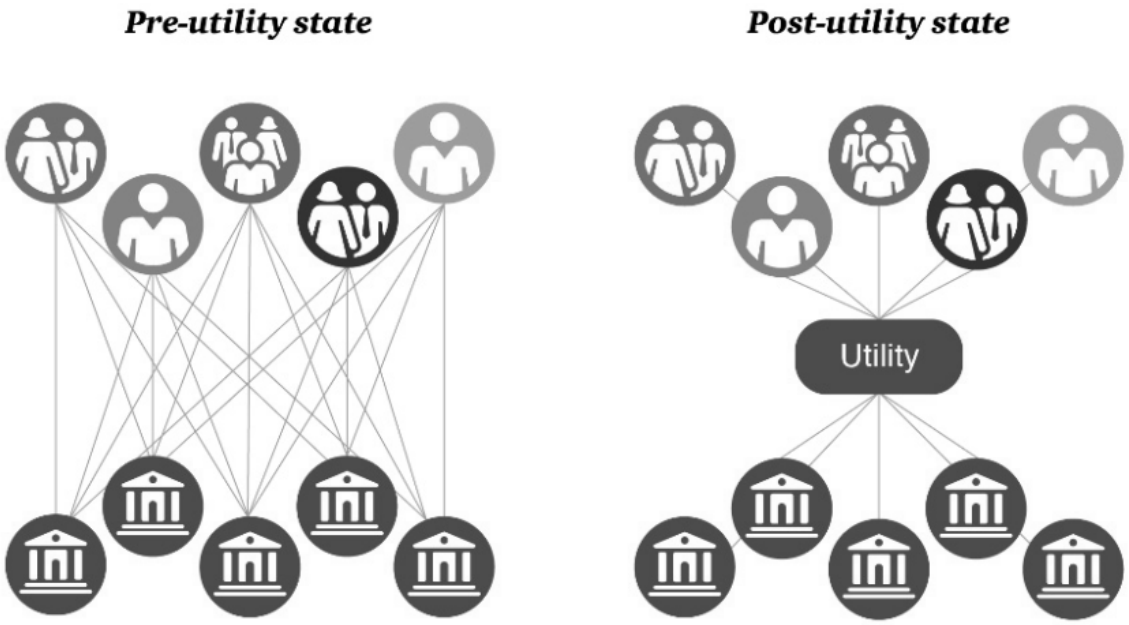

Рис. **Использование платформы для дистанционной идентификации устраняет дублирование идентификационных процедур**

Источник: Share and share alike: meeting compliance needs together with a KYC utility (PwC).

поддельных документов, необходима разработка соответствующих внутренних инструкций.

В-четвертых, дистанционная идентификация актуализирует риск вовлечения банка в сомнительные операции (отмывание доходов, финансирование терроризма). Дистанционная идентификация как возможность открыть банковский счет без личного обращения является благом для добросовестного клиента, так как экономит его время и упрощает документооборот. В то же время эти преимущества могут использоваться для обслуживания теневых схем отмывания доходов. В данном случае удаленная идентификация упрощает «расслоение» преступных доходов, так как технически появляется возможность открыть больше счетов в разных кредитных организациях. «На стадии расслоения лица, отмывающие деньги, стараются еще больше скрыть следы, по которым их могут обнаружить. Для этого одни сложные финансовые сделки наслаиваются на другие» [4]. Возможно и незаконное обналичивание денежных средств со счетов, открытых дистанционно, так как на сегодняшний день существуют технологии виртуальных банковских карт, технически возможно получить наличные денежные средства без физического присутствия банковской карты.

Таким образом, дистанционная идентификация клиента сопряжена с определенными рисками. Минимизации этих рисков способствуют мероприятия по надлежащей проверке клиентов (10-я рекомендация ФАТФ). Важно отметить, что чрезмерно жесткие требования по идентификации клиента и необоснованные мероприятия по надлежащей проверке клиента создают непреодолимый порог входа на рынок для потребителей [5]. В результате при отсутствии возможности пользоваться регулируемыми финансовыми продуктами может повышаться спрос на теневые финансовые услуги (в том числе расчеты наличными), что само по себе повышает риски ОД/ФТ. Именно цифровое взаимодействие с клиентом в процессе заключения договора способствует распространению регулируемых финансовых услуг, а значит, повышает прозрачность финансовой системы в целом.

Важно, что созданная Единая биометрическая система имеет потенциал платформы для дистанционной идентификации, а значит, может применяться во многих сферах, в том числе: разработка цифрового профиля гражданина, цифрового паспорта; создание платформы облачной квалифицированной электронной подписи; цифровые сервисы для участников избирательного процесса. Обзор мирового опыта применения биометрических технологий выявляет перспективы для использования биометрии, в том числе, в следующих сферах: банкинг и финансы в целом, биометрические платежи; транспортная инфраструктура (оплата проезда, пограничный контроль, авиаперевозки и т.д.); системы контроля и управления доступом [6].

Выводы и заключение

Подводя итог, следует еще раз подчеркнуть важность цифрового (дистанционного) взаимодействия с клиентом в процессе заключения договора. Технологическую основу для такого взаимодействия обеспечивает распространенность устройств для входа в Интернет (компьютер, планшет, смартфон) и проникновение Интернета, которое в РФ стабильно увеличивается и в 2019 г. превысило 75% взрослого населения. Среди преимуществ цифрового взаимодействия с клиентом: более быстрый и гибкий доступ к финансовым услугам; возможность заключать договоры значительно быстрее и дешевле; понижение стоимости обслуживания клиентов; высвобождение времени сотрудников и т.д. При дистанционном взаимодействии сохраняется необходимость идентификации и надлежащей проверки клиентов в соответствии с рекомендациями ФАТФ. Для решения этого вопроса в Российской Федерации создана Единая биометрическая система (ЕБС). После регистрации в ЕБС (фотография, запись голоса) пользователь получает возможность дистанционного открытия банковских счетов (при условии, что соответствующий банк предоставляет услугу дистанционного открытия банковских счетов). Таким образом, платформа ЕБС упрощает взаимодействие в процессе заключения договора как для клиента, так и для банка. Для клиента Единая биометрическая система — это возможность без личного обращения в банк открывать счета в банках с наилучшим обслуживанием и выгодными тарифами, для банка — это новый канал привлечения клиентов, экономия ресурсов при соблюдении нормативных требований по идентификации клиентов. Кроме того, Единая биометрическая система имеет потенциал платформы дистанционной биометрической идентификации, т.е. в будущем может использоваться не только для открытия банковских счетов, но и для идентификации участников любых других отношений. Платформа дистанционной идентификации важна как элемент инфраструктуры цифровой экономики, что безусловно перспективно для Российской Федерации.

Список источников

1. Достов В.Л., Емелин А.В. Совершенствование законодательства о ПОД/ФТ в части упрощенной идентификации клиентов. *Деньги и кредит.* 2014.(7):7–10.
2. Huang X. et al. A generic framework for three-factor authentication: Preserving security and privacy in distributed systems. *IEEE Transactions on Parallel and Distributed Systems*. 2011;22(8):1390–1397.
3. Сабанов А.Г., Смолина С.Г. Сравнительный анализ методов биометрической идентификации личности. *Труды Института системного анализа РАН.* 2016;66(3):11–20.
4. Ревенков П.В., Поспелов А.Л. Актуальные направления регулирования электронного банкинга. *Финансы и кредит.* 2015;(24)(648):2–13.
5. Достов В.Л., Шуст П.М., Козырева А.Д. Новые концепции применения риск-ориентированного подхода при осуществлении процедур идентификации. *Юридическая наука.* 2017;(5):16–21.
6. Емец М.И. Перспективы биометрической идентификации в контексте цифровой экономики Российской Федерации. *Креативная экономика.* 2019;13(5):927–936.

References

1. Dostov V.L., Emelin A.V. Improving AML/CFT legislation in terms of simplified customer identification]. *Dengi i kredit*. 2014;7:7–10. (In Russ.).
2. Huang X. et al. A generic framework for three-factor authentication: Preserving security and privacy in distributed systems. IEEE Transactions on Parallel and Distributed Systems. 2011;8(22):1390–1397.
3. Sabanov A.G., Smolina S.G. Comparative analysis of the methods of biometric identification of personality]. *Trudy instituta sistemnogo analiza Rossijskoj akademii nauk.* 2016;3(66):11–20. (In Russ.).
4. Revenkov P.V., Pospelov A.L. Actual directions of electronic banking regulation. *Finansy i kredit.* 2015;24:2–13. (In Russ.).
5. Dostov V.L., Shust P.M., Kozyreva A.D. New concepts of applying a risk-based approach in the implementation of identification procedures. *Yuridicheskaya nauka*. 2017;5:16–21. (In Russ.).
6. Emets M.I. Prospects of biometric identification in the context of the digital economy of the Russian Federation. *Kreativnaja ekonomika*. 2019;5(15):927–936. (In Russ.).