

РИСКИ УДАЛЕННОЙ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ КЛИЕНТА И ПУТИ ИХ СНИЖЕНИЯ**Василий Александрович ДАДАЛКО^а, Михаил Игоревич ЕМЕЦ^б**

^а доктор экономических наук, профессор кафедры анализа рисков и экономической безопасности, Финансовый университет при Правительстве РФ, Москва, Российская Федерация
antikrizis1@bk.ru
<https://orcid.org/0000-0001-5436-3286>
SPIN-код: 4287-0228

^б студент магистратуры, Финансовый университет при Правительстве РФ, Москва, Российская Федерация
memets@ya.ru
<https://orcid.org/0000-0002-1205-2735>
SPIN-код: 4483-1692

* Ответственный автор

История статьи:

Рег. № 191/2019
Получена 05.03.2019
Получена в доработанном виде 02.04.2019
Одобрена 16.05.2019
Доступна онлайн
15.11.2019

УДК 336.71
JEL: G21, O38

Ключевые слова:

идентификация клиента, отмыwanie доходов, финансирование терроризма, единая система идентификации и аутентификации, система межведомственного электронного взаимодействия

Аннотация

Предмет. Удаленная биометрическая идентификация клиентов – новый механизм для Российской Федерации, позволяющий заключать договоры без личного обращения потенциального клиента для идентификации. Этот механизм, с одной стороны, повышает доступность финансовых услуг, с другой – имеет определенные риски, в том числе в сфере ПОД/ФТ.

Цели. Обзор рисков и формулирование конкретных мероприятий, реализация которых поможет финансовым организациям минимизировать риски удаленной идентификации.

Методология. В работе использованы общенаучные и частно-научные методы, в том числе анализ и синтез, аналогия, сравнение, гипотетический метод.

Результаты. Исследована динамика становления института дистанционной идентификации в Российской Федерации, проведено сравнение различных методов идентификации клиента, проанализированы соответствующие риски и предложены мероприятия по их снижению.

Выводы. Удаленная (в том числе биометрическая) идентификация не создает принципиально новых рисков, но актуализирует уже имеющиеся. Данные риски известны банкам, применяющим технологии дистанционного обслуживания (ДБО) и имеющим портфель розничных кредитов. В условиях применения удаленной идентификации клиента повышается значимость десятой рекомендации ФАТФ «Надлежащая проверка клиентов». В рамках данной рекомендации финансовые организации должны предпринимать меры по установлению сведений в отношении потенциального клиента, а также проверять достоверность этих сведений на основе доверенных источников. Предложенные авторами мероприятия будут способствовать снижению актуализированных рисков при внедрении финансовыми организациями удаленной идентификации клиентов. Разработка направлений применения биометрической идентификации является принципиально важным вопросом, обуславливающим успех Единой биометрической системы.

© Издательский дом ФИНАНСЫ и КРЕДИТ, 2019

Для цитирования: Дадалко В.А., Емец М.И. Риски удаленной биометрической идентификации клиента и пути их снижения // Национальные интересы: приоритеты и безопасность. – 2019. – Т. 15, № 11. – С. 2057 – 2070. <https://doi.org/10.24891/ni.15.11.2057>

На международном уровне подходы уничтожения разрабатывает межправительственная к противодействию отмыwania доходов, организация – Группа разработки финансовых финансирования терроризма и мер борьбы с отмыwанием денег (ФАТФ). распространения оружия массового Основным методическим источником ФАТФ

по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения (ПОД/ФТ/ФРОМУ) являются 40 рекомендаций¹. Российская Федерация имплементировала в национальное законодательство все указанные рекомендации. Некоторые из них становятся особенно актуальными в контексте удаленной (биометрической) идентификации клиента. Например, 15-я рекомендация «Новые технологии» предусматривает обязательство стран и финансовых организаций оценивать новые технологии и продукты с точки зрения влияния на риски ОД/ФТ/ФРОМУ. Удаленная, в том числе биометрическая, идентификация – пример такой новой технологии, которая нуждается в оценке влияния на риски.

Цель статьи – обзор рисков и формулирование конкретных мероприятий, реализация которых поможет финансовым организациям минимизировать риски удаленной идентификации.

Актуальность темы обусловлена оказанием методологической поддержки созданию экосистемы цифровой экономики Российской Федерации, в которой обеспечено эффективное взаимодействие, включая трансграничное, бизнеса, научно-образовательного сообщества, государства и граждан, что является одной из целей программы «Цифровая экономика Российской Федерации»². Взаимодействие субъектов цифровой экономики становится более эффективным при наличии механизма удаленной идентификации. Специалисты по информационному праву по этому поводу отмечают, что в эпоху глобального информационного пространства высокая ценность удаленного доступа к сервисам и

знаниям не подвергается сомнению. В частности, текущий уровень развития информационных технологий позволяет участникам информационных отношений перевести значительную часть взаимоотношений в электронную форму, тем самым снижая транзакционные издержки и повышая эффективность использования человеческих ресурсов [1].

В соответствии с первой рекомендацией ФАТФ страны должны осуществлять оценку рисков и применять риск-ориентированный подход, чтобы мероприятия по ПОД/ФТ/ФРОМУ соответствовали выявленным рискам. В контексте идентификации клиента в российском законодательстве эта рекомендация отражается, в том числе, в различных подходах к идентификации клиента в зависимости от характера совершаемой операции и заключаемого договора.

По состоянию на 2018 г. российское законодательство предусматривает два вида удаленной идентификации. *Во-первых*, это упрощенная идентификация клиента – физического лица. Может проводиться удаленно с применением портала Госуслуги (ЕСИА) или системы межведомственного электронного взаимодействия (СМЭВ) для заключения некоторых видов договоров.

Во-вторых, это удаленная идентификация с применением биометрических технологий для открытия банковских счетов. В данной статье будут последовательно рассмотрены оба вида удаленной идентификации.

Несмотря на то, что некоторые исследователи [2] отмечают в том числе и терминологические недостатки в правовом регулировании, в целом законодательная база для удаленной идентификации сформирована. В 2014 г. в Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее – Закон № 115-ФЗ) было введено понятие «упрощенная идентификация клиента – физического лица» [3]. Упрощенная

¹ Международные стандарты по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения. Рекомендации ФАТФ. URL: <http://fedsfm.ru/content/files/documents/fatf/рекомендации%20fatf.pdf>

² Об утверждении программы «Цифровая экономика Российской Федерации»: расп. Правительства РФ от 28.07.2017 № 1632-р.

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 Закона № 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 идентификационных сведений о себе, а также СНИЛС, и/или ИНН, и/или номер полиса ОМС, а также номера мобильного телефона;
- 3) авторизация клиентом – физическим лицом в ЕСИА с подтвержденной учетной записью, указание предусмотренных идентификационных сведений и СНИЛС.

По логике законодателя проводить дистанционную упрощенную идентификацию по такой схеме можно в отношении клиентов, получающих услуги с относительно невысоким уровнем рисков ОД/ФТ/ФРОМУ. Именно поэтому в законе приводится исчерпывающий перечень случаев, когда упрощенная идентификация может проводиться, в том числе – при заключении договоров депозитарного и брокерского обслуживания при условии, что все расчеты осуществляются исключительно в безналичной форме по счетам, открытым в российской кредитной организации. Предполагалось, что закрепленное условие расчетов исключительно в безналичном порядке существенно снижает риски ОД/ФТ/ФРОМУ в случае дистанционной упрощенной идентификации, так как кредитная организация, открывшая счет, должна была ранее идентифицировать плательщика при личном обращении.

Технически упрощенная (удаленная) идентификация может выглядеть следующим

образом. При использовании для идентификации портала Госуслуги клиенту необходимо пройти авторизацию в Единой системе идентификации и аутентификации (ЕСИА), имея подтвержденную ранее учетную запись. В результате успешной авторизации потенциального клиента финансовая организация получает в распоряжение подтвержденные данные, необходимые для выполнения своей обязанности по идентификации. Преимущество данного метода – относительная простота для финансовой организации. Существенный недостаток заключается в том, что подтвержденную учетную запись на портале Госуслуги имеет далеко не все население, следовательно, не все потенциальные клиенты могут быть идентифицированы таким образом.

Процесс организации упрощенной (удаленной) идентификации клиента с использованием Системы межведомственного электронного взаимодействия (СМЭВ) технически более сложен для финансовой организации, и в этом состоит недостаток метода. Однако он может быть использован и для тех потенциальных клиентов, которые не имеют подтвержденной учетной записи на портале Госуслуги. Предназначение СМЭВ в данном случае заключается в подтверждении совпадения паспортных данных, указанных потенциальным клиентом, СНИЛС, и/или ИНН, и/или номера полиса ОМС. То есть если финансовая организация получила от государственных органов через СМЭВ подтверждение соответствия указанных паспортных данных и какого-либо второго идентификатора (СНИЛС, ИНН, номера полиса ОМС), клиент считается идентифицированным.

Практическая реализация механизма дистанционной упрощенной идентификации, по мнению авторов, не лишена определенных рисков.

Во-первых, существует группа технологических рисков, связанных с отказоустойчивостью баз данных ЕСИА и СМЭВ. Не исключена

ситуация, что из-за перегрузки серверы государственных органов не смогут оперативно или корректно обрабатывать запросы финансовых организаций. Методики оптимизации этого процесса должны реализовываться квалифицированными разработчиками. Разумеется, финансовая организация должна воздержаться от заключения договора с потенциальным клиентом в периоды неработоспособности ЕСИА и/или СМЭВ. При этом важно, что при таком способе идентификации происходит лишь проверка соответствия введенных данных. В этом заключается уязвимость перед мошенниками: теоретически легко представить ситуацию, когда мошенник, узнав паспортные данные и ИНН/СНИЛС жертвы, открывает дистанционно счет и получает возможность использовать его для ОД/ФТ/ФРОМУ.

Частично нивелирует этот риск запрос финансовой организацией скан-копии паспорта, что косвенно подтверждает физическое наличие документа у заявителя. Однако для мошенника не составит труда подделать скан-копию паспорта заявителя. Очевидные подделки должны выявляться при ручной обработке заявок с применением к таким заявителям ограничительных мер в виде запрета на дистанционное заключение договора. Еще больше минимизировать подобного рода риск поможет разрабатываемая Единая информационная система проверки сведений об абоненте³. Если законопроект будет принят, упрощенная (дистанционная) идентификация будет возможна только при подтверждении оператором принадлежности номера телефона заявителю. Существование этой системы возможно, так как операторы сотовой связи также являются организациями, осуществляющими операции с денежными

средствами и иным имуществом и обязаны идентифицировать клиентов в рамках регулирования Законом № 115-ФЗ.

Кроме перечисленных рисков, на сегодняшний день система упрощенной (удаленной) идентификации имеет определенные регуляторные пробелы, которые могут использоваться злоумышленниками в процессах ОД/ФТ/ФРОМУ. В частности, сущность брокерского и депозитарного договоров подразумевает переводы ценных бумаг, что особенно рискованно, если переводы ценных бумаг осуществляются с переходом права собственности. В таком случае счета, открытые злоумышленниками дистанционно, могут становиться транзитными, то есть использоваться для «запутывания следов» движения денежных средств и ценных бумаг. Для минимизации этого риска финансовые организации должны предусмотреть на уровне договоров с клиентами свое право на отказ в приеме в депозитарий ценных бумаг с переходом права собственности.

Во-вторых, счета «дистанционных» клиентов несут риск расчетов с использованием банковских счетов третьих лиц. В данной схеме брокерский счет, дистанционно открытый без ведома жертвы, может стать транзитным и использоваться для вывода денег на банковские счета третьих лиц с последующим обналичиванием. Для минимизации данного риска финансовым организациям следует на уровне договоров с клиентом предусмотреть свое право на отказ от расчетов с использованием банковских счетов третьих лиц. Обязательное наличие банковского счета, открытого на того же держателя «на входе» и «на выходе», позволяет снизить привлекательность дистанционного открытия счетов в некредитных финансовых организациях в целях реализации схем ОД/ФТ/ФРОМУ.

Описанные случаи упрощенной (дистанционной) идентификации распространяются только на определенные виды договоров, прямо предусмотренные

³ О внесении изменений в Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем и финансированию терроризма» и иные законодательные акты Российской Федерации (о создании информационной системы проверки сведений об абоненте): Законопроект № 514780-7. URL: <http://sozd.parliament.gov.ru/bill/514780-7>

нормами Закона № 115-ФЗ. Открытие банковского счета должно производиться при личном обращении клиента или его представителя для проведения идентификации с предоставлением оригиналов документов или надлежащим образом заверенных копий. Однако в 2018 г. вступил в силу Федеральный закон от 31.12.2017 № 482-ФЗ, вносящий изменения в ряд федеральных законов. Создан механизм, позволяющий идентифицировать граждан Российской Федерации дистанционно с применением биометрических технологий. Частный случай применения дистанционной биометрической идентификации – открытие банковских счетов без личного обращения клиента.

Физическому лицу потребуется всего лишь однажды пройти идентификацию уполномоченным банком при личном присутствии, пройти регистрацию в Единой системе идентификации и аутентификации (ЕСИА) и сдать биометрические образцы (фотография, запись голоса). Биометрические образцы будут переданы на хранение в созданную Единую биометрическую систему (ЕБС) на безвозмездной основе и с согласия клиента. В дальнейшем физическое лицо сможет открывать счета в банках уже без личного присутствия. Будет достаточно оставить заявку дистанционно, сопроводив ее собственной фотографией и записанным голосом в специальном приложении, а также пройдя авторизацию через ЕСИА на портале Госуслуг. В случае соответствия представленных в момент оформления дистанционной заявки биометрических образцов и хранящихся в Единой биометрической системе физическое лицо сможет воспользоваться финансовыми услугами без личного визита в банк.

Важно учесть мировой опыт открытия банковских счетов без личного обращения клиента. Например, банк HSBC во Франции предлагает дистанционное открытие банковского счета за 48 часов⁴. Для открытия

счета необходимо заполнить анкету, собственноручно подписать заявление, загрузить подтверждающие документы и пополнить счет с банковского счета, открытого на это же имя в другом французском банке. Таким образом, реализуется обязанность установления личности заявителя без личного обращения.

В США для граждан также доступна услуга дистанционного открытия банковских счетов. Например, Axos Bank в рамках процедур по надлежащей проверке клиентов использует информацию из бюро кредитных историй⁵. Эти примеры показывают, что развитые страны для дистанционного открытия счетов не используют биометрические технологии, а обходятся менее технологичными (и, следовательно, менее надежными) решениями. Однако в мире есть и практика применения биометрических технологий. Например, проект Aadhaar в Индии⁶, объединяющий информацию о более чем 1,3 млрд граждан и их биометрических данных. В данном случае используются радужка глаза и отпечатки пальцев.

В чем причина столь широкого распространения индийской государственной биометрической базы данных? Во-первых, это инициатива государства по регистрации граждан в данной системе, так как получение социальных услуг обусловлено наличием 12-значного Aadhaar-идентификатора. Во-вторых, это инициатива самих граждан, заинтересованных иметь постоянное удостоверение личности.

В Российской Федерации для получения государственных услуг используется Единая система идентификации и аутентификации, развита база данных Федеральной налоговой службы (ИНН) и Пенсионного фонда (СНИЛС), нет проблем с получением документов, удостоверяющих личность. То есть факторы, обусловившие успех индийской системы Aadhaar, отсутствуют в России. По

⁴ Open an Online Bank Account – Online Current Account. URL: <https://hsbc.fr/1/2/hsbc-france/particuliers/become-customer-open-account-online/>

⁵ Axos Bank / Enroll. URL: <https://enrollment.axosbank.com>

⁶ Home – Unique Identification Authority of India / Government of India. URL: <https://uidai.gov.in/>

этой причине, на наш взгляд, принципиально важным становится вопрос разработки направлений использования Единой биометрической системы помимо открытия банковских счетов без личного обращения. Если государство, бизнес и иные заинтересованные лица совместными усилиями не разработают направления для альтернативного использования Единой биометрической системы, эта инициатива может так и остаться на начальном этапе развития, а вложенные инвестиции не оправдают себя. При использовании биометрии процесс удаленного открытия счета усложняется, но ЕБС создает фундамент для использования этой инфраструктуры в цифровой экономике, например, для удаленного подписания договоров и иных документов, это так называемая «облачная электронно-цифровая подпись». Также потребуется продолжить совершенствование нормативно-правовой базы для распространения биометрической идентификации, в том числе – соответствующие изменения в федеральный закон «Об электронной подписи». В перспективе не исключено принятия самостоятельного федерального закона, регулирующего биометрическую идентификацию и сферы ее применения в экономике.

Ранее исследователями отмечалось, что «ни один из существующих методов не позволяет идентифицировать одного клиента из десятков и сотен тысяч без помощи дополнительных способов идентификации. Даже при всей уникальности биометрических данных биометрика идентифицирует личность лишь с определенной вероятностью. Поэтому применение биометрических систем в банках клиентов пока еще требует комплексного подхода в идентификации с применением классических инструментов» [4]. По этой причине в российской модели биометрической идентификации выбрана связка «ЕСИА + ЕБС», где авторизация в ЕСИА выступает в качестве аналога собственноручной подписи, а ЕБС обеспечивает гарантию того, что заявителем выступает именно та личность, на

которую зарегистрирована учетная запись в ЕСИА. Комбинация двух информационных систем обеспечивает приемлемый уровень надежности. Важен вопрос о типах биометрии, используемой для идентификации. Потенциально к используемым в данный момент двум видам идентификации (фото, запись голоса) могут добавиться и другие. Перспективен метод идентификации по радужной оболочке глаза, что объясняется возможностью сканирования на удаленном расстоянии, высокой информационной емкостью радужной оболочки глаза и т.д [5].

Подключение банка к Единой биометрической системе требует определенных затрат. По оценкам экспертов, первоначальные инвестиции составят 4 млн руб., далее – 130 тыс. руб. за каждое отделение⁷. Эти затраты включают в том числе программное обеспечение и средства криптографической защиты информации, соответствующие требованиям к безопасности. Это инвестиции, от которых можно ожидать отдачи в будущем в виде нового канала привлечения клиентов: дистанционное открытие счетов с использованием Единой биометрической системы.

Важно подчеркнуть, что регистрация клиентов в Единой биометрической системе – обязанность банков. При этом дистанционное открытие счетов – это их право, следовательно, если служба внутреннего контроля банка считает дистанционное открытие чрезмерно рискованной услугой, банк вправе принять решение не предоставлять такую услугу. При этом важно не допустить массового отказа банков от предоставления данной услуги, так называемый де-рискинг: «Чтобы снизить вероятность санкций со стороны регулятора, они отказываются от обслуживания целых сегментов аудитории, отдельных рынков или регионов, предпочитают не разрабатывать новые технологии. Де-рискинг может приводить к выталкиванию целых групп

⁷ Банки оценили биометрию.
URL: <https://kommersant.ru/doc/3731093>

потребителей к наличным расчетам или неофициальным финуслугам, что также негативно сказывается на эффективности национальной системы по ПОД/ФТ» [6].

На текущий момент система удаленной идентификации запущена, формируется база персональных биометрических данных в Единой биометрической системе. Газета «Ведомости» со ссылкой на оператора Единой биометрической системы ПАО «Ростелеком» отмечает, что на начало октября 2018 г. в системе зарегистрировалось лишь около 2 тыс. чел.⁸ (рис. 1).

Данный график был построен с помощью базового функционала программы MS EXCEL. В качестве исходных данных использовалась открытая информация СМИ о количестве регистраций. Пунктирная линия – трендовый прогноз, основанный на предположении, что динамика регистраций пользователей останется на прежнем уровне. Важно подчеркнуть ограниченную прогностическую способность такой модели, так как условия функционирования ЕБС могут меняться, как следствие – изменится динамика регистраций.

Главный вывод, который можно сделать из динамики регистрации пользователей – на начальном этапе база формируется медленно и при сохранении тренда ЕБС еще долго не сможет набрать «критическую массу» пользователей.

По состоянию на весну 2019 г. официальные данные о количестве зарегистрированных пользователей ЕБС не опубликованы, последние данные о количестве регистраций приводились газетой «Ведомости» осенью 2018 г.

Объяснить такую динамику начального этапа можно, с одной стороны, неготовностью многих банков предоставлять услугу регистрации в ЕБС, с другой стороны – невысоким интересом пользователей – действующих клиентов банков.

⁸ Банки оценили затраты на сбор биометрии граждан.
URL: <https://vedomosti.ru/finance/articles/2018/10/23/784463-banki-zatrati-na-biometrii-grazhdan>

Таким образом, потребуется некоторое время для формирования некой «критической массы» клиентов, прошедших очную идентификацию с предоставлением биометрических данных. Не исключено, что граждане просто не проявят должной заинтересованности, и ЕБС будет формироваться медленно, как медленно формировалась база ЕСИА. По состоянию на конец 2018 г. в ЕСИА зарегистрировано 86 млн пользователей⁹, при этом доля подтвержденных учетных записей в официальных публикациях не раскрывается. На формирование такой базы потребовалось около шести лет, при этом многие государственные структуры имеют показатели результативности деятельности, связанные с «проникновением» государственных услуг в электронном виде.

Каковы риски удаленной биометрической идентификации в целях открытия банковского счета? Прежде всего это *группа технологических рисков, связанных с технической реализацией системы удаленной идентификации*. В частности – 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 [7].

Не менее важной является *группа рисков мошенничества с поддельными документами и вовлечения финансовой организации в совершение сомнительных операций* (в том числе связанных с ОД/ФТ/ФРОМУ).

Во-первых, риск мошенничества с поддельными документами. Чтобы воспользоваться удаленной идентификацией, клиенту изначально необходимо зарегистрировать при участии уполномоченного банка образец изображения

⁹ Подведены итоги работы портала госуслуг за 2018 г.
/ Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций России.
URL: <https://digital.gov.ru/ru/events/38738/>

своего лица и запись голоса в Единой биометрической системе. Также необходимо наличие учетной записи ЕСИА, если ее нет – она будет создана уполномоченным банком. Именно здесь возникает риск мошенничества с документами: зная персональные данные, мошенник может вклеить свою фотографию в поддельный паспорт и зарегистрировать свои биометрические образцы от имени жертвы, а впоследствии – получить от имени жертвы кредиты в других банках без намерения возвращать.

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 поддельных документов, необходима разработка соответствующих внутренних инструкций. Кроме того, можно порекомендовать банкам использовать в этом процессе принцип «четырех глаз». Включение второго банковского сотрудника в данный процесс, во-первых, минимизирует операционные ошибки и повысит качество проверки документов, во-вторых, снизит риск коррупции персонала. При этом биометрия может в некоторых случаях снижать риск мошенничества. Например, при реализации определенных правил оценки клиента-заявителя. Среди примеров таких правил приводятся¹⁰:

- фотография в паспорте не совпадает с веб-фото клиента – подлог паспорта;
- веб-фото клиента совпадает с фотографией другого человека из базы – подлог паспорта;
- фотография клиента не совпадает с фотографиями на ранее поданных заявках с идентичными персональными данными – подмена фотографии, подмена персональных данных;

¹⁰ Горшков А. ЕБС или самостоятельные биометрические решения? Выбор есть // Расчеты и операционная работа в коммерческом банке. 2018. № 4(146).

- выявление идентичного лица в списке мошенников;
- выявление полностью идентичной фотографии в базе данных – внутреннее мошенничество.

Такая система может хорошо работать в больших масштабах – при условии накопления собственной базы данных фотографий заявителей и наличия алгоритмов их обработки.

Во-вторых, удаленная идентификация ускоряет и упрощает открытие счетов на имя номинальных владельцев, которые в дальнейшем не принимают участия в управлении счетами и передают данные для доступа бенефициарным владельцам. В данном случае удаленная идентификация упрощает «расслоение» преступных доходов, поскольку 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 [8]. Также счета могут использоваться недобросовестными лицами для обналичивания денежных средств через банкоматы. Отделам финансового мониторинга банков для минимизации данного риска можно порекомендовать устанавливать более жесткие лимиты на снятие наличных и переводы другим физическим лицам для клиентов, идентифицированных удаленно.

В-третьих, сотрудникам банков будет сложнее оценить реальные намерения потенциального клиента при открытии счета без личного контакта. При удаленной идентификации отсутствует возможность зафиксировать наличие бенефициарных владельцев у потенциальных клиентов, действующих от своего имени, но реально представляющих интересы иных лиц. В таком случае есть риск, что за номинальным держателем счета может скрываться,

например, фигурант перечня террористов или экстремистов. Отделам финансового мониторинга банков для минимизации данного риска можно порекомендовать уделять повышенное внимание мониторингу операций по счетам клиентов с признаком дистанционного открытия на предмет превышения заявленных при открытии объемов, несоответствия назначений платежа заявленным целям открытия счета. В работе [9] по этому поводу отмечается: «Служащий банка, руководство банка и (или) служба контроля должны осуществлять анализ обстоятельств любых необычных или подозрительных действий. В случае если рационального объяснения найти не удастся, могут быть приняты следующие решения:

- продолжать отношения с клиентом, обеспечив повышенный контроль;
- информировать власти о данном случае».

Впрочем, риски удаленной идентификации в сфере ОД/ФТ нельзя назвать новыми. Эти риски уже известны финансовым организациям, применяющим технологии дистанционного обслуживания, а также имеющим портфель розничных кредитов, где существуют риски кредитного мошенничества с использованием поддельных документов. То есть система удаленной идентификации не создает принципиально новых рисков в сфере ПОД/ФТ, а лишь актуализирует уже имеющиеся. Важно подчеркнуть, что услуга удаленного открытия банковского счета – это право, но не обязанность банков. При удаленной идентификации становится особенно актуальной десятая рекомендация ФАТФ – «Надлежащая проверка клиентов».

В соответствии с указанной рекомендацией финансовые организации обязаны принимать меры по надлежащей проверке клиента при установлении деловых отношений. Эта рекомендация имплементирована в российское законодательство, в том числе путем закрепления обязанности идентификации, получения информации о целях установления

деловых отношений, права принимать меры по определению источников происхождения денежных средств и т.д. Кроме того, п. 5.2. ст. 7 Закона № 115-ФЗ закрепляет право кредитных организаций отказаться от заключения договора или расторгнуть действующий договор при наличии подозрений о вовлечении клиента в ОД/ФТ/ФРОМУ. По мнению М.Ш. Магомедова и М.В. Каратаева, с помощью данной нормы была условно решена основная трудность предшествующего этапа развития системы внутреннего контроля в целях ПОД/ФТ, связанная с отсутствием у кредитных организаций реальных правовых инструментов управления риском вовлечения в процессы легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма [10]. Эта норма в полной мере применима к отношениям удаленной биометрической идентификации.

Таким образом, удаленная биометрическая идентификация – это новая технология, которая должна оцениваться государством и финансовыми организациями с точки зрения влияния на риски. В 2014 г. в российское законодательство был внедрен механизм упрощенной идентификации для заключения некоторых видов договоров (брокерского, депозитарного и т.д.) удаленно с применением информационных технологий. Для минимизации рисков вовлечения в ОД/ФТ/ФРОМУ при дистанционном заключении договора финансовой организации рекомендуется:

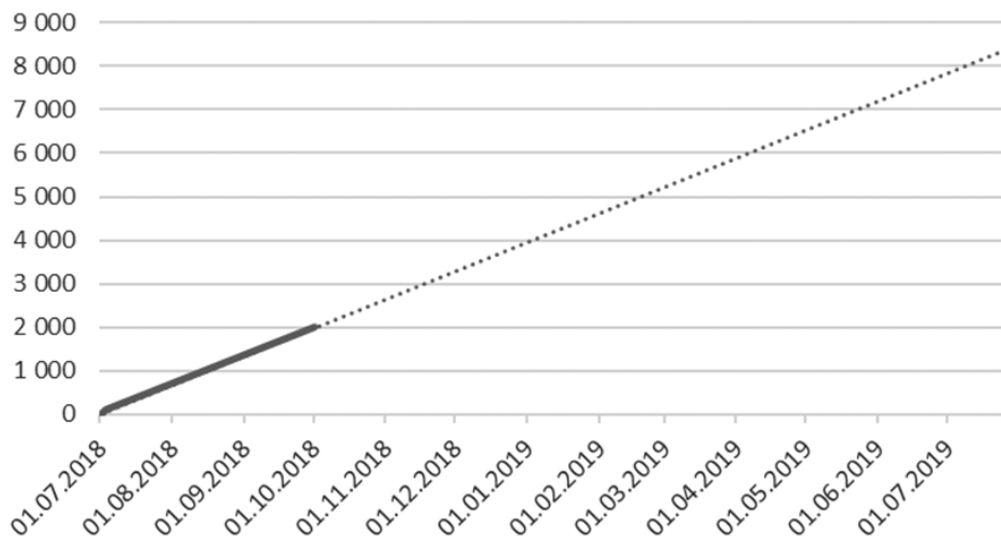
- запрашивать у клиента скан-копию паспорта и проводить обязательную ручную проверку для выявления очевидных подделок;
- предусмотреть на уровне договора с клиентом свое право отказа на ввод ценных бумаг в депозитарий с переходом права собственности, приобретенных не на организованных торгах;
- предусмотреть свое право на отказ от проведения расчетов с использованием банковских счетов третьих лиц.

С 2018 г. в российское законодательство внедрен механизм удаленной биометрической идентификации для дистанционного открытия банковских счетов. Подключение банка к Единой биометрической системе требует определенных затрат. Это инвестиции, от которых можно ожидать отдачи в будущем в виде получения нового канала привлечения клиентов: дистанционное открытие счетов. Важно, что открытие счета с применением удаленной биометрической идентификации – это право, но не обязанность банка. Отделы финансового мониторинга при дистанционном открытии счетов вправе принимать любые обоснованные и доступные в сложившихся обстоятельствах меры для надлежащей проверки клиентов. Для минимизации рисков, связанных с удаленной идентификацией, рекомендуется:

- проводить обучение сотрудников, регистрирующих клиентов в ЕСИА и ЕБС, выявлению поддельных документов, разрабатывать и регулярно обновлять соответствующие инструкции;
- применять принцип «четырёх глаз» при регистрации клиентов в ЕСИА и ЕБС для снижения операционных ошибок и коррупции персонала;

- устанавливать более жесткие лимиты (кредитный, на снятие наличных, переводы другим физическим лицам) для клиентов, идентифицированных удаленно;
- уделять повышенное внимание мониторингу операций на предмет превышения заявленных при открытии объемов, несоответствия назначений платежа заявленным целям открытия счета.

Применение удаленной биометрической идентификации в финансовой сфере – это только одно из возможных направлений развития. Ст. 14.1. «Применение информационных технологий в целях идентификации граждан Российской Федерации» Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» заложила правовую базу для распространения удаленной биометрической идентификации на любые сферы экономики. Какие именно сферы экономики получат дополнительное развитие при внедрении цифровых идентификационных технологий – перспективная тема для последующих исследований.

Рисунок 1**Количество регистраций пользователей в ЕБС****Figure 1****The number of customer registrations in the Unified Biometric System**

Примечание. Пунктирная линия – трендовый прогноз.

Источник: составлено авторами на основе материалов СМИ

Source: Authoring based on mass media materials

Список литературы

1. Наумов В.Б., Брагинец А.Ю. Информационно-правовые проблемы удаленной идентификации субъектов в сфере финансовых услуг // Информационное право. 2016. № 1. С. 13–19.
2. Наумов В.Б. Problems of Development of Legislation on Identification of the Subjects of Information Space in Digital Economy // Труды Института государства и права РАН. 2018. № 4. С. 125–150. URL: <https://cyberleninka.ru/article/n/problems-of-development-of-legislation-on-identification-of-the-subjects-of-information-space-in-digital-economy>
3. Достов В.Л., Емелин А.В. Совершенствование законодательства о ПОД/ФТ в части упрощенной идентификации клиентов // Деньги и кредит. 2014. № 7. С. 7–10.
4. Винокуров А. Биометрические системы идентификации в кредитных организациях как инструмент противодействия мошенничеству // Финансы и кредит. 2016. Т. 22. Вып. 21. С. 15–23. URL: <https://cyberleninka.ru/article/n/biometricheskie-sistemy-identifikatsii-v-kreditnyh-organizatsiyah-kak-instrument-protivodeystviya-moshennichestvu>
5. Петров И.В., Минакова Н.Н. Сравнительный анализ методов некооперативного распознавания радужной оболочки глаза // Известия АлтГУ. 2016. № 1. С. 163–167. URL: <https://cyberleninka.ru/article/n/sravnitelnyy-analiz-metodov-nekooperativnogo-raspoznavaniya-raduzhnoy-obolochki-glaza>
6. Достов В.Л., Шуст П.М., Козырева А.Д. Новые концепции применения риск-ориентированного подхода при осуществлении процедур идентификации // Юридическая наука. 2017. № 5. С. 104–112. URL: <https://cyberleninka.ru/article/n/novye-kontseptsii-primeneniya-risk-orientirovannogo-podhoda-pri-osuschestvlenii-protsedur-identifikatsii>

7. *Сабанов А.Г., Смолина С.Г.* Сравнительный анализ методов биометрической идентификации личности // Труды Института системного анализа РАН. 2016. Т. 66. № 3. С. 11–20.
8. *Ревенков П.В., Поспелов А.Л.* Актуальные направления регулирования электронного банкинга // Финансы и кредит. 2015. Т. 21. Вып. 24. С. 2–13.
URL: <https://cyberleninka.ru/article/n/aktualnye-napravleniya-regulirovaniya-elektronnogo-bankinga>
9. *Ревенков П.В., Дудка А.Б., Воронин А.Н., Каратаев М.В.* Финансовый мониторинг: управление рисками отмывания денег в банках. М.: КноРус, 2012. 280 с.
10. *Магомедов М.Ш., Каратаев М.В.* ФАТФ: первые 25 лет в архитектуре международных отношений. Сообщение 1. Эволюция концепции финансового мониторинга // Вестник РАЕН. 2014. № 3. С. 25–30.

Информация о конфликте интересов

Мы, авторы данной статьи, со всей ответственностью заявляем о частичном и полном отсутствии фактического или потенциального конфликта интересов с какой бы то ни было третьей стороной, который может возникнуть вследствие публикации данной статьи. Настоящее заявление относится к проведению научной работы, сбору и обработке данных, написанию и подготовке статьи, принятию решения о публикации рукописи.

RISKS OF USER'S REMOTE BIOMETRIC IDENTIFICATION AND OPTIONS TO MITIGATE THEM**Vasilii A. DADALKO ^{a,*}, Mikhail I. EMETS ^b**^a Financial University under Government of Russian Federation, Moscow, Russian Federation
antikrizis1@bk.ru
<https://orcid.org/0000-0001-5436-3286>^b Financial University under Government of Russian Federation, Moscow, Russian Federation
memets@ya.ru
<https://orcid.org/0000-0002-1205-2735>

* Corresponding author

Article history:Received 5 March 2019
Received in revised form
2 April 2019
Accepted 16 May 2019
Available online
15 November 2019**JEL classification:** G21, O38**Keywords:** user identification, money laundering, terrorist financing, unified identification and authentication system, interdepartmental electronic interaction system**Abstract****Subject** Remote biometric identification is a new mechanism for the Russian Federation. It streamlines the contractual work without being personally present to be identified. On the one hand, the mechanism makes financial services more accessible, but, on the other hand, it is exposed to certain risks, including the money laundering and financing of terrorism.**Objectives** The study overviews risks and formulates specific actions, which would help financial institutions mitigate remote identification risks.**Methods** We applied general scientific and particular methods, including analysis and synthesis, analogy, comparison, hypothetical method.**Results** We investigated the pace at which the remote identification practice devolves in Russia and compared various methods of user identification, analyzing respective risks and suggesting actions to reduce them.**Conclusions and Relevance** Remote (biometric) identification does not engender any absolutely new risks, but revitalizes the existing ones. Banks are aware of the risks as they run remote servicing technologies and have a portfolio of retail customers. As long as remote identification is used, FATF Recommendation 10 – *Customer Due Diligence* becomes more significant. As part of Recommendation 10, financial institutions should undertake customer due diligence measures and verify the information through reliable sources. The proposed actions will reduce the arising risks, when financial institutions implement the remote identification practice with respect to their customers. It is critical to outline aspects of biometric identification, since it contributes to the successful use of the Unified Biometric System.

© Publishing house FINANCE and CREDIT, 2019

Please cite this article as: Dadalko V.A., Emets M.I. Risks of User's Remote Biometric Identification and Options to Mitigate Them. *National Interests: Priorities and Security*, 2019, vol. 15, iss. 11, pp. 2057–2070.
<https://doi.org/10.24891/ni.15.11.2057>**References**

1. Naumov V.B., Braginets A.Yu. [Information and legal problems of remote identification of subjects in the field of financial services]. *Informatsionnoe pravo = Informational Law*, 2016, no. 1, pp. 13–19. (In Russ.)
2. Naumov V.B. Problems of Development of Legislation on Identification of the Subjects of Information Space in Digital Economy. *Trudy Instituta gosudarstva i prava Rossiiskoi akademii nauk = Proceedings of the Institute of State and Law of Russian Academy of Sciences*, 2018, no. 4, pp. 125–150. URL: <https://cyberleninka.ru/article/n/problems-of-development-of-legislation-on-identification-of-the-subjects-of-information-space-in-digital-economy>

3. Dostov V.L., Emelin A.V. [The improvement of AML/CFT legislation in part of simplified customer identification requirements]. *Den'gi i kredit = Money and Credit*, 2014, no. 7, pp. 7–10. (In Russ.)
4. Vinokurov A. [Biometric identification systems in credit institutions as an anti-fraud tool]. *Finansy i kredit = Finance and Credit*, 2016, vol. 22, iss. 21, pp. 15–23.
URL: <https://cyberleninka.ru/article/n/biometricheskie-sistemy-identifikatsii-v-kreditnyh-organizatsiyah-kak-instrument-protivodeystviya-moshennichestvu> (In Russ.)
5. Petrov I.V., Minakova N.N. [A comparative analysis of non-cooperative iris recognition techniques]. *Izvestiya of AltGU = Izvestiya of Altai State University*, 2016, no. 1, pp. 163–167.
URL: <https://cyberleninka.ru/article/n/sravnitelnyy-analiz-metodov-nekooperativnogo-raspoznavaniya-raduzhnoy-obolochki-glaza> (In Russ.)
6. Dostov V.L., Shust P.M., Kozyreva A.D. [New concepts of applying a risk-based approach as part of identification procedures]. *Yuridicheskaya nauka = Legal Science*, 2017, no. 5, pp. 104–112. URL: <https://cyberleninka.ru/article/n/novye-kontseptsii-primeneniya-risk-orientirovannogo-podhoda-pri-osuschestvlenii-protsedur-identifikatsii> (In Russ.)
7. Sabanov A.G., Smolina S.G. [Comparative analysis of the methods of biometric identification of personality]. *Trudy Instituta sistemnogo analiza Rossiiskoi akademii nauk = Proceedings of the Institute for Systems Analysis of Russian Academy of Sciences*, 2016, vol. 66, no. 3, pp. 11–20. (In Russ.)
8. Revenkov P.V., Pospelov A.L. [Regulating electronic banking: Current issues]. *Finansy i kredit = Finance and Credit*, 2015, vol. 21, iss. 24, pp. 2–13.
URL: <https://cyberleninka.ru/article/n/aktualnye-napravleniya-regulirovaniya-elektronnogo-bankinga> (In Russ.)
9. Revenkov P.V., Dudka A.B., Voronin A.N., Karataev M.V. *Finansovyi monitoring: upravlenie riskami otmyvaniya deneg v bankakh* [Financial monitoring: Money laundering risk management in banks]. Moscow, KnoRus Publ., 2012, 280 p.
10. Magomedov M.S., Karataev M.V. [FATF: The first 25 years in architecture of international relations message 1. Evolution of the concept of financial monitoring]. *Vestnik Rossiiskoi akademii estestvennykh nauk = Bulletin of Russian Academy of Natural Sciences*, 2014, no. 3, pp. 25–30. (In Russ.)

Conflict-of-interest notification

We, the authors of this article, bindingly and explicitly declare of the partial and total lack of actual or potential conflict of interest with any other third party whatsoever, which may arise as a result of the publication of this article. This statement relates to the study, data collection and interpretation, writing and preparation of the article, and the decision to submit the manuscript for publication.