Дата поступления рукописи в редакцию: 17.07.2026 г. DOI: 10.24412/2224-9133-2026-7-380-384
Дата принятия рукописи в печать: 31.07.2026 г.

ДМИТРИЕВА София Дмитриевна,
студент, Финансовый университет при Правительстве РФ,
e-mail: Sofya.sona2004@yandex.ru

ПАТРУШЕВА Ольга Денисовна,
студент, Финансовый университет при Правительстве РФ,
e-mail: odpatrusheva@mail.ru

КИРСАНОВА Дарья Максимовна,
студент, Финансовый университет при Правительстве РФ,
e-mail: kisanova2015@yandex.ru

ПРИМЕНЕНИЕ РИСК-ОРИЕНТИРОВАННОГО ПОДХОДА В ОНЛАЙН-БАНКИНГЕ: РЕГУЛИРОВАНИЕ И ПРАКТИКА

Аннотация. *В настоящее время онлайн-банкинг подвержен двум ключевым рискам: использованию в целях отмывания доходов и финансирования терроризма. В данной статье авторы анализируют эффективность применения риск-ориентированного подхода для минимизации данных рисков. Исследование проводилось с опорой на международные акты финансового регулирования и надзора, а также на исследования, рассматривающие успешность существующего законодательства в этой сфере.*

Ключевые слова: *банковская деятельность, онлайн-банкинг, риск-ориентированный подход, ФАТФ, противодействие легализации отмывания доходов, клиент банка.*

DMITRIEVA Sofia Dmitrievna,
student, Financial University under the Government of the Russian Federation

PATRUSHEVA Olga Denisovna,
student, Financial University under the Government of the Russian Federation

KIRSANOVA Daria Maksimovna,
student, Financial University under the Government of the Russian Federation

APPLYING A RISK-BASED APPROACH TO ONLINE BANKING: REGULATION AND PRACTICE

Annotation. *Online banking is exposed to two major risks: its utilisation for the purposes of money laundering and the financing of terrorism. This article examines the effectiveness of applying a risk-based approach to mitigate these risks. The study is founded upon international legal instruments pertaining to financial regulation and supervision, as well as scholarly works evaluating the effectiveness of extant legislation in this domain.*

Key words: *banking, online banking, risk-based approach, FATF, countering the legalization of money laundering, bank client.*

Мир стремительно трансформируется, всё больше аспектов нашей жизни перемещаются в цифровое пространство. Вместе с этим растет популярность онлайн-банкинга, что представляет собой способ управления финансами через интернет. Как отмечает Ручкина Г. Ф., цифровые банки и онлайн-банкинг стремительно развиваются, и по некоторым оценкам годовой темп их роста в период с 2024 по 2028 г. составит 13 - 15% [1, с. 15]. При этом использование таких сервисов несёт в себе не только положительный аспект, но и ряд угроз, которые требуют детального рассмотрения.

Однако вместе с этими преимуществами появляются и серьёзные риски. Среди рисков, с которыми сталкиваются банки при использовании интернет-банкинга, можно выделить: операционные, репутационные, риски безопасности, стратегические, кредитные, рик онлайн-мошенничества и иные [2, с. 169]. Эти риски, существовавшие и ранее, после внедрения цифровизации трансформировались и требуют нового подхода со стороны банков.

Самой острой проблемой остаётся деятельность злоумышленников, использующих высокие технологии для кражи персональных данных. Современные мошенники постоянно совершенствуют свои методы,для того чтобы обойти защитные механизмы банков и пользователей.

Также не следует забывать и про технический аспект. Несмотря на значительные усилия банков по защите своих систем, технические сбои остаются реальностью. Они могут возникать по разным причинам: ошибки в программном коде, перегрузка серверов или целенаправленные атаки. Такие ситуации могут привести к временному отключению услуг, задержкам в проведении транзакций или даже потере важных данных. Особенно критичны такие проблемы в моменты, когда клиенту требуется срочный доступ к своим средствам.

Риск-ориентированный подход в онлайн-банкинге - это метод управления рисками, который предполагает выявление, устранение или ослабление потенциального влияния источников банковских рисков для повышения надежности банковской деятельности. Данный подход предлагает гибкое и соразмерное распределение ресурсов в зависимости от уровня потенциальной угрозы, а также дает возможность финансовым институтам эффективно выполнять предъявляемые к ним требования: обеспечивать беспрепятственный пользовательского опыта, соблюдать требования по противодействию легализации доходов и финансированию терроризма (ПОД/ФТ), а также защищать свою деловую репутацию в условиях постоянно эволюционирующего поля киберугроз и изощренных мошеннических схем.

Необходимо учитывать, что онлайн-банкинг может быть уязвим ко многим факторам, связанным с безопасностью удаленных операций. В отличие от традиционных отделений банков, где банковское обслуживание носит личный характер и специалист может полагаться на невербальные сигналы, онлайн-сервисы требуют компенсировать риски новыми, более технологичными способами. Это вызывает особую озабоченность, когда поставщики услуг базируются в юрисдикциях, где на них может не распространяться надлежащее регулирование и надзор в области ПОД/ФТ. Среди наиболее значимых рисков, на которые должен быть направлен риск-ориентированный подход, можно выделить:

риски, связанные с удаленной идентификацией, включающие в себя возможность использования поддельных или похищенных удостоверений личности. Это делает процесс онбординга критически важным, особенно когда речь идет про применение усиленных мер проверки (Enhanced Due Diligence, EDD) для клиентов из юрисдикций с повышенным риском или вовлеченных в политически значимые должности (PEP).

высокая скорость и анонимность операций, может способствовать осуществлению транзакций, направленных на легализацию средств, полученных преступным путем, поскольку цифровые платежи могут быть проведены мгновенно и через несколько стран, существенно затрудняя их отслеживание для органов финансового мониторинга без наличия продвинутых аналитических инструментов.

угрозы кибербезопасности и компрометации учетных данных, что напрямую напрямую влияет на риски ПОД/ФТ, так как в случае получения несанкционированного доступа к учетной записи клиента злоумышленники могут использовать ее для проведения мошеннических операций и отмывания денег, маскируя их под легитимную активность законного владельца счета.

Риск-ориентированный подход включает в себя идентификацию, анализ и оценку рисков, касающихся предоставления банковских услуг в сети Интернет. Данное благополучно сказывается на функционировании банков и финансовых институтов, так как позволяет эффективно распределять ресурсы для минимизации возможных убытков и обеспечения безопасности операций.

Ключевые элементы риск-ориентированного подхода:

Выявление рисков. Одним из самых важных этапов является обнаружение возможных проблем и уязвимых мест, которые способны причинить вред для онлайн-банкинга.

Оценка рисков. Необходимо изучить вероятность возникновения какой-либо угрозы и оценить возможные масштабы ущерба, который мо-

жет быть нанесен посредством этого риска.

Управление рисками. После анализа рисков происходит разработка и внедрение способов и мер для их снижения. В это будет входить использование передовых технологий защиты данных, регулярное обновление программного обеспечения и обучение пользователей правилам безопасности.

Контроль и отчетность. Необходимо систематически проводить мониторинг ситуации с рисками, выявлять насколько эффективны принятые меры.

Одним из методов управления рисками в интернет-банкинге является создание всестороннего контроля за безопасностью. Он включает в себя установку авторизационных привилегий, логический и физический контроль доступа, обеспечение безопасности инфраструктуры.

Также для управления рисками в интернет-банкинге можно использовать идентификацию личности и авторизацию клиентов. Для этого в современном мире используется множество способов. Например, пароли, смарт-карты, биометрические и цифровые сертификаты. Еще одним способом управления рисками в интернет-банкинге является использование методов идентификации транзакций. Данное будет обеспечивать безотказность работы и устанавливать возможность идентификации электронных банковских транзакций.

Применение риск-ориентированного подхода в онлайн-банкинге эффективно благодаря его универсальности. Такой подход служит защите кредитных организаций и их клиентов от любых угроз их интересам или негативных явлений независимо от степени развития законодательной базы банковской деятельности. Так, например, для борьбы с отмыванием доходов и финансированием терроризма разработаны как международные, так и национальные меры, основанные на риск-ориентированном подходе.

В целях борьбы с отмыванием доходов была создана Группа разработки финансовых мер борьбы с отмыванием денег (далее - «ФАТФ»), членом которой Россия является с 2003 года. Несмотря на то, что членство в ней было приостановлено, ее система по борьбе с отмыванием денег и финансированием терроризма продолжают соответствовать всем стандартам [3].

Риск-ориентированный подход (РОП) имеет решающее значение для эффективной реализации пересмотренных Международных стандартов ФАТФ по противодействию отмыванию денег и финансированию терроризма и распространению оружия массового уничтожения, которые были приняты в 2012 году.

Как следует из Руководства по риск-ориентированному подходу для банковского сектора, выпущенного в 2021 году, при предотвращении кибератак на мобильный банкинг означает, что банки, финтех-компании, поставщики платежных услуг, должны выявлять, оценивать, а также понимать риски кибератак, которым они подвержены, и разрабатывать меры по предотвращению этих рисков, чтобы эффективно их смягчить [4].

Особенно интересны в отношении онлайн-банкинга Рекомендации 16, которые вводят определение «электронного перевода», а также требования касающиеся как внутренних, так и трансграничных электронных переводов, которые касаются как фиатных валют, так и виртуальных активов.

Отправляющие, а также в некоторых случаях и получающие учреждения, обязаны собирать информацию об отправителях и получателях. Как следует из Пояснительной записки к Рекомендациям, такая информация включает в себя: имя и номер счета отправителя, адрес отправителя или номер государственного идентификационного документа, или идентификационный номер клиента, или дату и место рождения, имя получателя и его номер счета.

Таким образом, ФАТФ требует, чтобы все клиенты проходили надлежащую проверку, в том числе при осуществлении электронных переводов. Названные данные позволяют идентифицировать как отправителя, так и получателя, что обеспечивает прозрачность переводов, даже если они осуществляются без открытия банковского счета.

При подозрении на осуществление запрещенной операции банк имеет право попытаться уменьшить риски, в том числе отклонив или заблокировав операцию. Все финансовые учреждения, если они подозревают или имеют основания подозревать, что средства являются доходом от преступной деятельности или связаны с финансированием терроризма, обязаны оперативно сообщать о своих подозрениях в соответствующие регуляторы. Это следует из Рекомендаций 20. С одной стороны, это создает дополнительную административную нагрузку на банки и другие финансовые учреждения, с другой - гарантирует, что государственные органы остаются в курсе всех подозрительных операций, информация о которых может способствовать раскрытию финансовых преступлений.

Российская Федерация достигла определенных успехов в сфере борьбы с отмыванием доходов и финансированием терроризма. Так, в 2019 России удалось получить пятое место по эффективности своей системы с данными проблемами в мире, что демонстрировало успехи в борьбе с отмыванием средств [5]. Этот успех был закреплен оценкой экспертов в 2023 году. Тем не менее, в связи с санкционным давлением после начала

специальной военной операции, в феврале 2023 г. членство России в ФАТФ было приостановлено. Несмотря на это, Россия продолжает добросовестно выполнять свои обязательства.

Основной федеральный закон, который в России регламентирует применение риск-ориентированного подхода - это Федеральный закон от 07.08.2001 N 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

Согласно нему, под осуществлением внутреннего контроля понимается реализация организациями, осуществляющими операции с денежными средствами или иным имуществом, правил внутреннего контроля, включающая в себя в том числе выполнение требований законодательства по идентификации клиентов, по проведению в установленных случаях упрощенной идентификации клиентов - физических лиц, по оценке степени риска совершения клиентами подозрительных операций и отнесению клиентов к группам риска совершения подозрительных операций.

Как следует из данного федерального закона, кредитные организации должны самостоятельно разрабатывать документацию, согласно которой они будут классифицировать риски на уровне внутреннего контроля. Так, в Указании № 3624-У отмечено, что система управления рисками и капиталом должна выявлять присущие, потенциальные и значимые для банков риски [6].

В Информационном письме Росфинмониторинга от 18.03.2009 № 2 «О порядке применения Федерального закона от 07.08.2001 № 115-ФЗ» указано, что организации обязаны самостоятельно оценивать степень риска на основании признаков операций, видов и условий деятельности, имеющих риск совершения клиентами операций в целях легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма [7]. При этом должны учитываться и внутренние признаки, которые были установлены самой организацией в рамках внутреннего контроля. Такими признаками могут быть:

любая деятельность, связанная с интенсивным оборотом наличности;

отсутствие информации о клиенте (юридическом лице, в том числе кредитной организации) в официальных справочных изданиях, а также невозможность осуществить связь с клиентом по указанным им адресам и телефонам;

наличие в деятельности клиента подозрительных операций, сведения по которым представлялись в уполномоченный орган и др.

При этом, как следует из ст. 7 данного федерального закона, кредитные организации и филиалы иностранных банков обязаны относить каждого клиента к одной из следующих групп риска:

низкая степень (уровень) риска совершения подозрительных операций;

средняя степень (уровень) риска совершения подозрительных операций;

высокая степень (уровень) риска совершения подозрительных операций

Уровень риска в отношении каждого клиента указывается в его анкете. Если хотя бы один из факторов из Приложения 5 оценивается как повышенный, уровень риска клиента повышается. Также существует перечень операций, контроль которых обязателен. В отношении онлайн-банкинга такому контролю подвержены:

переводы денежных средств, если отправляющей или получающей стороной является лицо с местом регистрации/проживания в стране, не входящей в ФАТФ и/или не выполняющей ее требований;

операции с цифровыми финансовыми активами;

операции, совершаемые по поручению иностранного гражданина, на сумму, равную или превышающую 50 000 рублей либо равную или ее эквиваленту в иностранной валюте и др.

Таким образом, нормы ФАТФ находят свое отображение в российском законодательстве, которое предъявляет достаточно высокие требования к банкам и другим учреждениям при осуществлении онлайн операций. Несмотря на то, что это имеет свои преимущества, которые позволяют эффективно предотвращать подозрительные переводы, у такого строгого подхода есть недостатки.

Одним из главных недостатков является большое количество ложных блокировок. Алгоритмы искусственного интеллекта исследуют счета для определения подозрительных транзакций. И если какая-то сделка покажется системе «нестандартной», велика вероятность блокировки счета без предварительных разбирательств. Это вызывает трудности, которые заставляют людей обращаться в службу поддержки для разрешения проблемы.

Также велик процент случаев, когда клиенты становятся частью мошеннической цепи, сами того не подозревая. Злоумышленники часто используются доверием граждан в своих планах, делая их непреднамеренными участниками противоправных действий. К примеру, они могут потребовать перевести на указанный ими счет денежные средства, поступившие гражданину от третьего лица. Клиент лично переводит средства на указанный счет, не подозревая, что его данные используют для отмывания денег через/с помощью счета. В подобных случаях операция может быть ошибочно классифицирована как подозрительная, хотя никакого злого умысла у клиента не было. Банковские системы, основанные на риск-

ориентированном подходе, могут заблокировать его аккаунт, что усложняет процесс.

Отметим, что несмотря на свою популярность, для достаточно большого количества людей онлайн-банкинг остается инструментом, которому они не доверяют, в том числе из-за риска стать жертвой мошенников [8].

Риск-ориентированный подход играет важную роль в защите финансовых систем от мошенничества и киберугроз. Однако его недостатки, такие как частые ошибочные блокировки, шаблонные алгоритмы и автоматизация, могут создавать серьезные неудобства для клиентов. Особенно сложными являются случаи, когда законопослушный гражданин становится жертвой мошенников или ошибочной блокировки.

Таким образом, риск-ориентированный подход в онлайн-банкинге демонстрирует высокую эффективность в выявлении и предотвращении угроз связанных с мошенническими операциями и не только. Комплексный подход позволит минимизировать риски и обеспечить доверие пользователей к цифровым финансовым сервисам. При этом меры безопасности не должны вести к несправедливому ограничению в доступе к финансовым услугам и продуктам со стороны финансовых учреждений.

Список литературы:

[1] Ручкина Г. Ф. Цифровые банки на рынке банковских услуг: необходимость правового регулирования деятельности // Banking Law. - 2024. - № 04. - С. 14-21- DOI: 10.18572/1812-3945-2024-4-14-2..

[2] Хафизова Р. Х. Риски цифрового банкинга // Экономика и бизнес: теория и практика. - 2022. - № 5-3. - С. 168-170. - DOI: 10.24412/2411-0450-2022-5-3-168-170..

[4] FATF (2021), Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris, www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-VASP.html..

[5] ФАТФ (2019) «Отчет о взаимной оценке мер по борьбе с отмыванием денег и финансированием терроризма, Российская Федерация» // ФАТФ, Париж https://www.fatf-gafi.org/content/dam/fatf-gafi/mer/Mutual - Evaluation-Russian - Federation - декабрь 2019.

[6] Указание Банка России "О требованиях к системе управления рисками и капиталом кредитной организации и банковской группы" от 15.04.2015 г. № 3624-У // Вестник Банка России. - 15.06.2015 г. - № 51. - с изм. и допол. в ред. от 06.10.2023.

[7] Информационное письмо «О порядке применения Федерального закона от 07.08.2001 N 115-ФЗ» от 18.03.2009 № 2 // URL: https://www.consultant.ru/document/cons_doc_LAW_67213/..

[8] РБК. Более половины россиян сочли рискованным использование онлайн-банкинга // РБК. — URL: https://www.rbc.ru/rbcfreenews/6420f14a9a79472ecdb9a69f (дата обращения: 25.10.2023).

References:

[1] G.F. Ruchkina. Digital banks in the banking services market: the need for legal regulation of activities // Banking Law. - 2024. - № 04. - S. 14-21- DOI: 10.18572/1812-3945-2024-4-14-2..

[2] Hafizova R. Kh. Risks of digital banking // Economics and business: theory and practice. - 2022. - № 5-3. - S. 168-170. - DOI: 10.24412/2411-0450-2022-5-3-168-170..

[4] FATF (2021), Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris, www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-VASP.html..

[5] FATF (2019) "Report on the mutual assessment of measures to combat money laundering and terrorist financing, Russian Federation "// FATF, Paris https://www.fatf-gafi.org/content/dam/fatf-gafi/mer/Mutual - Evaluation-Russian - Federation - December 2019.

[6] Bank of Russia Ordinance No. 15.04.2015 // Bank of Russia Bulletin, dated 3624-U, On Requirements for the Risk and Capital Management System of a Credit Institution and a Banking Group. - 15.06.2015 - No. 51. - with rev. and additional as amended by 06.10.2023.

[7] Information letter "On the Procedure for Application of Federal Law dated 07.08.2001 No. 115-FZ" dated 18.03.2009 No. 2 // URL: https://www.consultant.ru/document/cons_doc_LAW_67213/..

[8] WCB. More than half of Russians considered it risky to use online banking // RBC. - URL: https://www.rbc.ru/rbcfreenews/6420f14a9a79472ecdb9a69f (access date: 25.10.2023).