ФИНАНСЫ

Н.Г. СИНЯВСКИЙ
доктор экономических наук, доцент, ведущий научный сотрудник
ФГБУН Институт экономической политики и проблем
экономической безопасности Факультета экономики и бизнеса
Финансового университета при Правительстве Российской Федерации

РИСКИ ВНЕДРЕНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ ДЛЯ ПРОТИВОДЕЙСТВИЯ ОТМЫВАНИЮ ДЕНЕГ: ИДЕНТИФИКАЦИЯ, РАНЖИРОВАНИЕ И МЕРЫ ИХ РЕГУЛИРОВАНИЯ[1]

Цифровые продукты потенциально могут сделать операции противодействия отмыванию денег и финансированию терроризма менее затратными, более эффективными и существенно ускорить их реализацию, обеспечить качественное соблюдение стандартов Группы разработки финансовых мер борьбы с отмыванием денег и улучшить межстрановое взаимодействие. Появляется возможность для финансовых организаций предоставить услуги большему количеству экономических субъектов. Поэтому мировая система противодействия отмыванию денег широко внедряет инновационные цифровые технологии для обеспечения оперативной и достоверной информации о субъектах экономической деятельности и проводимых ими операциях за счет существенного увеличения объема обрабатываемых данных. Однако их применение сопряжено с рисками системного характера. Целью исследования является идентификация рисковых факторов и мер их регулирования, а также их систематизация и ранжирование по важности, что может служить основанием для соответствующего распределения ресурсов, используемых для воздействия на рисковые факторы. Уровень рисков, рисковые факторы и меры их регулирования оцениваются на основе опросов авторитетных организаций, исследований специалистов и нормативных документов.

Ключевые слова: *противодействие отмыванию денег, Группа разработки финансовых мер по борьбе с отмыванием денег (ФАТФ), цифровизация, риски.*

УДК: 336.025

EDN: LTKMAC

DOI: 10.52180/2073-6487_2025_5_167_187

[1] Статья подготовлена по результатам исследований, выполненных за счет бюджетных средств по государственному заданию Финансового университета при Правительстве Российской Федерации.

Введение

Система противодействия отмыванию (легализации) денег, финансированию терроризма и финансированию распространения оружия массового уничтожения (сокращенно ПОД/ФТ/ФРОМУ[2]) решает задачи «установления стандартов и содействия эффективному применению правовых, регулирующих и оперативных мер по борьбе с отмыванием денег, финансированием терроризма и финансированием распространения оружия массового уничтожения, а также с иными связанными угрозами целостности международной финансовой системы»[3]. Российская система противодействия в организационном плане является подсистемой международной системы и действует в соответствии с положениями, принятыми Группой разработки финансовых мер борьбы с отмыванием денег (ФАТФ)[4]. В настоящее время ФАТФ взяла курс на «…“умное” регулирование финансового сектора»[5], стимулирующее инновации в сфере цифровых технологий. Технологический уровень информационных (цифровых) технологий (ИТ), используемых российской системой противодействия, соответствует общему технологическому уровню, достигнутому в мире, с его достоинствами и недостатками.

Целью настоящей работы является идентификация рисковых факторов внедрения цифровых технологий в ПОД и мер их регулирования, разработка рекомендаций по распределению усилий по реализации этих мер на основе упорядочения системных рисков. *Соответственно, объектом исследования являются риски организационного и тех-*

---

[2] Далее в тексте ПОД/ФТ/ФРОМУ будет называться системой противодействия отмыванию денежных средств (системой противодействия).

[3] Международные стандарты по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения. Рекомендации ФАТФ (обновлено в феврале 2025 г.). С. 7. https://www.cbr.ru/content/document/file/174972/fatf_rec_ru.pdf (дата обращения: 23.08.2025).

[4] Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ) является независимой межправительственной организацией, разрабатывающей и популяризирующей свои принципы для защиты всемирной финансовой системы от угроз отмывания денег, финансирования терроризма и финансирования распространения оружия массового уничтожения. Рекомендации ФАТФ являются общепризнанными международными стандартами по противодействию отмыванию денег и финансированию терроризма (ПОД/ФТ). Подробная информация о ФАТФ размещена на сайте: www.fatf-gafi.org.

[5] Возможности и проблемы новых технологий для ПОД/ФТ // ФАТФ. Париж, Франция, 2021. С. 7. https://www.fatf-gafi.org/content/dam/fatf-gafi/translations/guidance/Russian-Opportunities-and-Challenges-of-New-Technologies-for-AML-CFT.pdf (дата обращения: 23.08.2025).

нологического характера, сопутствующие внедрению цифровых технологий российской системой противодействия отмыванию денег.

Проблема анализа и оценки рисков внедрения цифровых технологий в процедуры российской системы ПОД в настоящее время очень актуальна. *Во-первых*, потому, что мировая система ПОД/ФТ сегодня перестраивается в процессе внедрения риск-ориентированного подхода на основе цифровизации, а современный этап развития российской экономики происходит на фоне широкомасштабного внедрения цифровых технологий. «Новые технологии должны повысить скорость, качество или эффективность и снизить стоимость некоторых мер ПОД/ФТ, а также снизить затраты на повсеместное внедрение системы ПОД/ФТ по сравнению с использованием традиционных методов и процессов»[6]. Новации позволят конкретизировать процесс ПОД, концентрируя усилия на отслеживании опасных объектов и избегая ущемление прав законопослушных граждан. Данный тезис поддерживается и на уровне ООН. Так, Резолюция Совета Безопасности ООН S/RES/2322 (2016) «Об укреплении международного правоохранительного и судебного сотрудничества в борьбе с терроризмом» прямо призывает государства-члены обмениваться информацией, включая биометрические и биографические данные, об иностранных боевиках-террористах (ИБТ) и других отдельных террористах и террористических организациях[7]. При этом «Правительствам необходимо учитывать последствия применения этой технологии для прав человека, чтобы защитить тех, кого идентифицируют такие системы, от злоупотреблений и обеспечить, чтобы действия, предпринимаемые на этапе планирования и впоследствии, осуществлялись в соответствии с обязательствами по международному праву, закрепленными в международных и региональных документах по правам человека»[8].

«Стандарты ФАТФ были пересмотрены с целью ужесточения требований к ситуациям более высокого риска, чтобы позволить странам принимать целевые меры в тех областях, где остаются более высокие риски и должны быть предприняты дополнительные шаги. Страны должны сначала определить, оценить и понять риски отмывания денег и финансирования терроризма, с которыми они сталкиваются, и затем принять соответствующие меры по устранению этих рисков. Риск-ориентированный подход позволяет странам в рамках требова-

---

6 Там же. С. 6.

7 United Nations Compendium of Recommended Practices For the Responsible Use and Sharing of Biometrics in Counter Terrorism // Compiled by CTED and UNOCT. 2018. P. 7. https://www.unodc.org/pdf/terrorism/Compendium-Biometrics/Compendium-biometrics-final-version-LATEST_18_JUNE_2018_optimized.pdf (дата обращения: 23.08.2025).

8 Там же. P. 7.

ний ФАТФ гибко применять набор мер для того, чтобы более эффективно распределить свои ресурсы и принять превентивные меры, соответствующие характеру рисков, с целью концентрации своих усилий самым эффективным образом»[9].

«Одной из основных проблем, препятствующих эффективной реализации мер ПОД/ФТ, является плохое понимание угроз и рисков ОД/ФТ. Решения, принимаемые на основе ненадлежащих оценок рисков, иногда бывают неточными и неактуальными, поскольку в значительной степени определяются человеческим фактором и обусловлены «защитным» формальным подходом к риску, а не истинным риск-ориентированным подходом»[10]. Формальный подход, не учитывающий особенности идентифицируемых объектов, заставляет усиливать регуляторные требования.

Во-вторых, цифровизация – это инновации, и их внедрение сопряжено с высоким риском.

По мнению А.Н. Козырева [1, с. 5], самыми популярными исследованиями цифровой экономики являются работы Д. Тапскотта [2; 3]. *Главным достижением цифровой экономики Д.* Тапскотт, основываясь на теоретических положениях Р. Коуза [4], считает *уменьшение трансакционных издержек.* Однако он предсказывал и появление проблем, связанных с развитием новых технологий: «… новые технологии могут нарушить … конфиденциальность…, растет разрыв между цифровыми богатством и бедностью, … растет цифровое неравенство на международном и национальном уровнях» [5]. Последующее развитие событий показало, что рисковый спектр внедрения ИТ гораздо шире.

Новизна настоящей статьи заключается в выявлении и упорядочении рисковых факторов внедрения цифровых технологий системой противодействия отмыванию денег, генерируемых организацией внедрения и использованием информационных технологий, и мер воздействия на них, *что позволяет сформулировать рекомендации по распределению усилий, направляемых на регулирование рисков.*

Поскольку речь идет о внедрении новаций, то ожидать большого количества структурированной информации для исследования не приходится. «Потенциал и возможные последствия многих из этих

[9] Международные стандарты по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения. Рекомендации ФАТФ (обновлено в феврале 2025 г.). С. 8. https://www.cbr.ru/content/document/file/174972/fatf_rec_ru.pdf (дата обращения: 23.08.2025).

[10] Возможности и проблемы новых технологий для ПОД/ФТ // ФАТФ. Париж, Франция, 2021. С. 11. https://www.fatf-gafi.org/content/dam/fatf-gafi/translations/guidance/Russian-Opportunities-and-Challenges-of-New-Technologies-for-AML-CFT.pdf (дата обращения: 24.08.2025).

новых технологий до сих пор не изучены в достаточной степени»[11]. Тем не менее на основе доступных данных здесь делается попытка дать количественную оценку уровня рисков, сопровождающих инновационные процессы в российской системе противодействия отмыванию денег, на основе которой упорядочиваются по важности рисковые факторы и формулируются предложения по распределению усилий на реализацию мер по их регулированию.

Исследователи цифровых технологий считают, что наилучшие перспективы для внедрения – у искусственного интеллекта (ИИ). От внедрения цифровых новаций ожидают: снижения субъективизма и расширения области используемой информации; возможности анализа больших объемов неструктурированных данных; облегчения выбора программных продуктов; расширения возможностей «электронного правительства». Сегодня имеются положительные результаты использования новаций для задач противодействия, но называются и риски их внедрения: ошибки обработки данных, особенно при увеличении объема информации; возможности использования новаций преступниками; нарушения прав человека; сопротивление рекомендациям; недостаток специалистов и неподготовленность руководителей компаний; опасность кибератак; высокая стоимость реализации новаций; затруднения использования новаций малым бизнесом.

Материалы, используемые для анализа рисков, и методы исследования

В исследовании применяется системный подход к анализу рисков использования цифровых технологий при решении задач по совершенствованию деятельности национальной системы ПОД/ФТ[12]. Анализируются общесистемные риски мировой системы противодействия. Для систематизации рисков применяется риск-ориентированный подход, означающий (в узком смысле) оценку важности рисков и сосредоточение усилий по их регулированию на наиболее важных рисках. Такой подход снижает уровень неопределенности ситуации, позволяет использовать дополнительную информацию для принятия решений, не распылять ресурсы, предназначенные для регулирования

[11] Возможности и проблемы новых технологий для ПОД/ФТ // ФАТФ. Париж, Франция, 2021. С. 6. https://www.fatf-gafi.org/content/dam/fatf-gafi/translations/guidance/Russian-Opportunities-and-Challenges-of-New-Technologies-for-AML-CFT.pdf (дата обращения: 24.08.2025).

[12] Концепция развития национальной системы противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма. 30.05.2018 // Сайт Президента России. http://www.kremlin.ru/supplement/5310 (дата обращения: 24.08.2025).

рисков. Данный подход широко используется в российской практике государственного управления. При этом «…контролирующий орган посещает объект только в случае потенциального нарушения требований, при срабатывании индикатора риска. Такая практика снижает административную нагрузку на предпринимателей. Развитием риск-ориентированного подхода в рамках реформы контрольной (надзорной) деятельности занимается Минэкономразвития России при поддержке Правительства РФ»[13]. В настоящей работе также делается попытка выявления и упорядочения рисков и мер их регулирования.

Для анализа используются данные опросов авторитетных организаций и результаты исследований. Возможность использования международного (в том числе и российского) опыта для анализа цифровых новаций в российской системе противодействия обусловлена тем, что организация противодействия отмыванию денег во всем мире представляет единую систему, организована по единым стандартам, а также и тем, что организация российской подсистемы котируется в мире очень высоко и вносит существенный вклад в работу мировой системы противодействия. Так как опросы не позволяют оценить риск непосредственно, то оценка делается косвенно – по результатам внедрения и опросных оценок проектов. Предполагается, что уровень риска выше, если реализация проекта оказалась проблемной, проект не получил широкого распространения или считается менее перспективным. Уровень риска того или иного атрибута внедрения оценим долей респондентов, отметивших этот атрибут в качестве проблемного при внедрении цифровых технологий в ПОД/ФТ.

Результаты исследования общесистемных рисков

Применение ИТ для противодействия отмыванию денег сопряжено с рисками регулятивного или операционного характера[14]. Оценим общие риски противодействия, характерные для мировой системы ПОД/ФТ. Уровень рисков и меры регулирования определим на основании опросов авторитетных организаций и данных ФАТФ,

[13] Министерство экономического развития Российской Федерации. В первом квартале Минэк согласовал более 30 новых индикаторов риска. https://www.economy.gov.ru/material/news/v_pervom_kvartale_minek_soglasoval_bolee_30_novyh_indikatorov_riska.html (дата обращения: 24.08.2025).

[14] *Grint R., O'Driscoll C., Paton S.* New Technologies and Anti-Money Laundering Compliance // Financial Conduct Authority. London, 2017. P. 34. http://www.fca.org.uk/publication/research/new-technologies-in-aml-final-report.pdf (дата обращения: 24.08.2025).

где указаны результаты опроса о «трудностях и проблемах, связанных с разработкой и/или внедрением новых технологий»[15].

Рассмотрим факторы рисков и возможные меры воздействия на них. Расположим риски в порядке убывания их уровня, который оценим долей опрошенных, отмечающих данный аспект как проблему внедрения новых технологий[16].

Первый, наибольший риск отмечается *в регулировании процедур противодействия* (уровень риска 68%, т. е. доля респондентов, отметивших сложности регулирования как трудность внедрения ИТ). В качестве факторов этого риска можно отметить низкий уровень интерпретируемости и объясняемости, низкий уровень стандартизации, неуверенность в надежности данных, обработанных с использованием новых технологий. Субъекты, деятельность которых регулируют, не обладают достаточными компетенциями для оценки параметров цифровых технологий и для обоснования необходимости их применения. Недостаточно компетенций и у регуляторов, что усложняет надзор.

По опросам ФАТФ «52% респондентов определили SupTech и RegTech как области противодействия отмыванию денег, где от новых технологий можно получить больше всего преимуществ»[17]. Опросы Cambridge Centre for Alternative Finance при поддержке Ernst&Young[18] среди регуляторов показали следующие оценки частоты использования цифровых продуктов в RegTech-проектах регуляторов в перспективе (сумма частот использования продуктов в 2019 г. и прогноза частоты будущего расширения использования) (табл. 1).

Ранее нами было высказано предположение, согласно которому уровень риска тем выше, чем менее распространена технология или инструмент. В соответствии с этим предположением в таблице технологии и инструменты упорядочены таким образом, что наиболее рискованной технологией является роботизация, а наименее рискованной – машинное обучение.

---

[15] Возможности и проблемы новых технологий для ПОД/ФТ. ФАТФ. Париж, Франция. 2021. С. 36. https://www.fatf-gafi.org/content/dam/fatf-gafi/translations/guidance/Russian-Opportunities-and-Challenges-of-New-Technologies-for-AML-CFT.pdf (дата обращения: 24.08.2025).

[16] Там же. С. 36.

[17] Там же. С. 21.

[18] *Schizas E., McKain G., Zhang B.Z., Garvey K., Ganbold A., Hussain H., Kumar P., Huang E., Wang S., Yerolemou N.* The Global RegTech Industry Benchmark Report // Cambridge Centre for Alternative Finance (CCAF). Cambridge, 30.06.2019. P. 41. http://dx.doi.org/10.2139/ssrn.3560811. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3560811 (дата обращения: 25.08.2025).

Таблица 1

Частота использования цифровых технологий и инструментов, используемых компаниями RegTech, %

Технологии и инструменты	Использование в 2019 г.	Рассматривается возможность использования в будущем	Прогнозная частота
Машинное обучение	56	16	72
Глубокое обучение	33	12	45
Облачные вычисления	66	1	67
Прогностическая аналитика данных	43	14	57
Обработка естественного языка	35	9	44
Протоколы передачи данных	40	3	43
Семантика (графический анализ)	32	9	41
Робототехника	30	6	36

Источник: составлено автором по данным CCAF (*Schizas E., McKain G., Zhang B.Z., Garvey K., Ganbold A., Hussain H., Kumar P., Huang E., Wang S., Yerolemou N.* The Global RegTech Industry Benchmark Report // Cambridge Centre for Alternative Finance (CCAF). Cambridge, 30.06. 2019. С. 41. http://dx.doi.org/10.2139/ssrn.3560811. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3560811 (дата обращения: 25.08.2025)).

Для оценки диапазона уровня рисков использования цифровых технологий отметим, что, по опросам «Делойт»[19], 63% компаний сообщают об отсутствии сотрудников, обладающих компетенциями по роботизации. Опросы НИУ ВШЭ[20] показали, что 50% компаний, использующих ИИ, указали на дефицит специалистов в этой области. То есть можно утверждать, что недостаток компетенций отмечается у 50–63% компаний. «Несмотря на потенциальные преимущества инновационных технологий, человеческий фактор по-прежнему является основой успеха органов ПОД/ФТ. Наличие достаточного количества сотрудников с необходимыми навыками, опытом и квалификацией имеет решающее значение для достижения этими органами своих целей»[21].

[19] Тенденции развития роботизации в РФ – RPA. 2020. Deloitte. С. 9. https://ru.readkong.com/page/tendencii-razvitiya-robotizacii-v-rf-deloitte-7047445 (дата обращения: 26.08.2025).

[20] Практики и перспективы внедрения технологий ИИ. 15 ноября 2024 г. Пресс-служба ИСИЭЗ НИУ ВШЭ. https://www.novostiitkanala.ru/news/detail.php?ID=181118 (дата обращения: 26.08.2025).

[21] SupTech applications for AML. BIS. 2019. FSI Insights. No. 8. P. 16. https://www.bis.org/fsi/publ/insights18.pdf (дата обращения: 27.08.2025).

Все это обусловливает высокую зависимость результатов инноваций от политики надзорных органов и ограничивает возможности новых технологий. Возникают сложности в формировании методик оценки эффективности цифровых технологий и рисков противодействия. Процедуры работы с данными существенно ускоряются, что заставляет быстрее принимать решения по выявлению преступлений. Все это создает проблемы для противодействия[22].

В качестве управляющего воздействия для снижения риска регулирования важно участие аккредитованных ИТ-компаний в обучении студентов ИТ-специальностей, разработка новых образовательных программ, привлечение преподавателей-практиков из индустрии, обучение преподавателей и руководителей образовательных программ в сфере ИТ. Целесообразна организация автоматической обратной связи, чтобы подконтрольные субъекты в реальном времени видели полезность предоставляемой регуляторам информации. Повышению эффективности регулирования будет способствовать разработка регуляторами специальных руководств и обмен информацией между подконтрольными субъектами. Также можно предложить использование материалов реальных дел для машинного обучения вместо копирования действий сотрудников. Так или иначе, основной задачей повышения результативности регулирования является задача реализации всех преимуществ новых технологий регулируемыми субъектами и способность эти преимущества показать регуляторам. Так, денежно-кредитным управлением Сингапура было выпущено руководство по определению области аналитики ПОД/ФТ, где сотрудничество частного и государственного секторов может принести существенные выгоды[23].

В качестве второго по важности риска назовем *риск нарушения требования о защите данных и неприкосновенности личной жизни*. Уровень этого риска 56%. Проблемы регулирования таких рисков рассмотрены в Guidance on Digital[24]. Предлагается для оценки приемлемости процедуры идентификации субъектов установить степень надежности технологии, архитектуры и управления системы цифрового удостоверения в аспекте использования для незаконных операций. Принципы организации

---

[22] Возможности и проблемы новых технологий для ПОД/ФТ // ФАТФ. Париж, Франция, 2021. С. 47. https://www.fatf-gafi.org/content/dam/fatf-gafi/translations/guidance/Russian-Opportunities-and-Challenges-of-New-Technologies-for-AML-CFT.pdf (дата обращения: 27.08.2025).

[23] Industry Perspectives – Adopting Data Analytics Methods for AML/CFT. MAS, 2018. Pp. 21–22. https://www.mas.gov.sg/-/media/mas/regulations-and-financial-stability/industry-perspectives--adopting-data-analytics-methods-for-amlcft.pdf (дата обращения: 27.08.2025).

[24] Guidance on Digital ID // FATF. Paris, 06.03.2020. https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html (дата обращения: 27.08.2025).

цифровой идентификации представлены в Principles On Identification[25]. Это обеспечение инклюзивности (отсутствие дискриминации), надежности технологии, обеспечивающей достоверность идентификации и защиту данных, обратной связи от идентифицируемых субъектов.

Следующим по важности, по мнению ФАТФ, является *риск низкого качества данных* (уровень риска 44%). Факторами такого риска являются: низкая гармонизация данных; необходимость для новых систем дополнительной настройки и адаптации к требованиям разных юрисдикций; сложность коммуникаций регулируемых субъектов внутри их стран, а также и межстрановых коммуникаций. Кроме того, проблемой является влияние ошибок самих создателей средств ИИ, что может проявляться во многих процессах. Влияет на качество данных также высокая скорость обработки и проведения операций, усложняющая получение качественной информации[26]. В качестве мер регулирования такого риска можно предложить оптимизацию участия человека в проверке достоверности данных. В частности, может широко использоваться трансляция в цифровой вид текстов на естественном языке, служащих исходной информацией для анализа.

Уровень *технологического риска* составляет 42%. Источники такого риска в том, что надзорные стратегии не соответствуют новым технологиям, а разработчики технологий, в свою очередь, не обладают компетентностью в понимании особенностей государственного управления. Также процесс государственных закупок может оказаться слишком долгим по сравнению с динамикой обновления технологий. Нельзя исключать и возможности того, что требования потребителей окажутся не выгодны разработчикам (пример – пожелание эксклюзивности), а новые технологии окажутся не настолько эффективными, как предполагают контрольные органы или конкретный представитель этих органов, принимающий решение о целесообразности инноваций. Возможны, кроме того, трудности интеграции новых технологий в устаревшие системы или отсутствие технических возможностей для использования новых технологий. В этих случаях можно применять такую специальную меру воздействия на технологические риски, как совершенствование надзорных стратегий.

[25] Principles on Identification for Sustainable Development: Toward the Digital Age (English). World Bank. Washington, D.C. 2022. http://documents.worldbank.org/curated/en/213581486378184357/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age (дата обращения: 27.08.2025).

[26] Возможности и проблемы новых технологий для ПОД/ФТ // ФАТФ. Париж, Франция, 2021. С. 47. https://www.fatf-gafi.org/content/dam/fatf-gafi/translations/guidance/Russian-Opportunities-and-Challenges-of-New-Technologies-for-AML-CFT.pdf (дата обращения: 27.08.2025).

Близким по содержанию к технологическому риску является *риск сложности внедрения новых технологий* (уровень риска 39%.). Источники такого риска в основном совпадают с источниками технологического риска. В качестве специального фактора можно выделить отсутствие технических возможностей для надлежащего использования новых технологий. Кроме того, уровень квалификации сотрудников регуляторов, как правило, не позволяет разобраться в содержании цифровых технологий и осуществлять эффективный надзор за их применением. Решение проблемы сложности внедрения можно ожидать на пути применения универсальных мер регулирования общесистемных рисков.

Уровень *риска стоимости новых информационных технологий* оценивается в 37%. Кроме собственной стоимости новаций существенное влияние на стоимость оказывают следующие факторы. Это трудность интегрирования новых технологий в устаревшие системы, т. к. технологии стареют и требуют дополнительных вложений в новые решения. Из-за низкой гармонизации данных широкое распространение новаций может оказаться дорогим. Закупка новых технологий является сложным и долгим процессом. Также может оказаться, что масштабное использование новых технологий возможно только при наличии существенных материальных стимулов. Результативной мерой регулирования стоимостного риска новых информационных технологий также может стать нематериальное стимулирование (требования об обязательном использовании ИТ либо большая степень доверия между регуляторами и контролируемыми субъектами).

Следующим системным *риском* является *неприятие риска* (уровень риска 18%). Возможно, что неприятие риска вызывают: трансляция человеческих ошибок в программные продукты; сложность оценки рисков; скорость обработки данных. Факторами этого риска для малых организаций являются: сложность в оценке результативности цифровых технологий; возможность невыполнения требований в сфере ПОД/ФТ; нарушения неприкосновенности личной жизни. Процедуры регулирования данного риска, видимо, стоит строить на основе решения задачи минимизации участия людей в формировании массивов информации.

Еще один *риск – отсутствие регулятивной песочницы*[27] *для апробирования новых технологий* (уровень риска 15%). Данный риск реализуется

[27] «Регулятивные песочницы – это особый набор правил, который позволяет инновационным компаниям протестировать свои продукты и услуги в ограниченной среде, без риска нарушения финансового законодательства». (Регулятивные песочницы. Регулирование как сервис // Ассоциация участников рынка электронных денег и денежных переводов «АЭД». 2016. С. 5. https://web.archive.org/web/20200211072642/

вследствие несоответствия новых технологий ожиданиям регуляторов или конкретных контролеров. При этом сложным является разработка показателей оценки с учетом скорости операций. Очевидной мерой регулирования данного риска является создание стандартного инструмента для испытания новых технологий.

Риск неудовлетворения коммерческих интересов (уровень риска 13%) во многом связан с масштабностью использования новых технологий, которая может стать невозможной из-за недостаточной гармонизации данных. Для такого риска также важна проблема критериев оценки результативности технологий[28].

Риск угрозы вмешательства со стороны преступников (уровень риска 11%) возникает из-за возможностей, которые открывают новые технологии для преступников, а также из-за опасностей, связанных с преступным использованием особенностей обращения с финансовыми услугами пожилыми людьми, жителями сельской местности или далеких от городов регионов. Предполагается, что возможности регулирования рисков несоблюдения коммерческих интересов и преступного вмешательства будут возрастать с ростом успешности применения универсальных мер регулирования общесистемных рисков.

Важным риском в социальной сфере является *риск невозможности охвата всех слоев населения финансовыми услугами и отказа от обслуживания клиентов во избежание рисков*. Уровень этого риска оценивается в 7%. Невысокий уровень оценки такого риска объясняется большим вниманием, которое уделяется социальным проблемам, связанным с внедрением цифровых технологий. Среди факторов такого риска можно отметить возможность лишения доступа к финансовым услугам категории лиц, имеющих ограниченный доступ к финансовому обслуживанию, которая увеличивается в том случае, если не используется риск-ориентированный подход в ходе идентификации личности. Быстрое проведение операций также является фактором, усиливающим данный социальный риск[29]. В качестве меры регулирования данного риска можно отметить обеспечение инклюзивности инструментов цифровой идентификации как в плане исполнения,

http://www.npaed.ru/images/downloads/Regulatory_sandbox_AED_Report2016.pdf (дата обращения: 27.08.2025).)

[28] Возможности и проблемы новых технологий для ПОД/ФТ // ФАТФ. Париж, Франция, 2021. С. 45. https://www.fatf-gafi.org/content/dam/fatf-gafi/translations/guidance/Russian-Opportunities-and-Challenges-of-New-Technologies-for-AML-CFT.pdf (дата обращения: 27.08.2025).

[29] Там же. С. 47.

так и использования[30,31,32]. Причем здесь важна минимизация ошибок идентификации до приемлемого уровня[33]. Кроме того, важно решать проблемы социального, процедурного и правового характеров. При этом целесообразна организация специальной работы с людьми, имеющими ограниченный доступ к финансовым услугам[34]. Как указывалось ранее, проблемы финансовой изоляции и сохранности личной информации рассмотрены в Guidance on Digital ID[35], а принципы создания и эксплуатации систем цифровой идентификации изложены в Principles On Identification[36].

Наконец, в список наиболее важных системных рисков (уровень риска 3%) включается *риск нерезультативности сведений о подозрительных операциях* (СПО). Действенной мерой регулирования такого риска является использование разработанных в России и рекомендованных для внедрения в других странах личных кабинетов[37] для информирования о полезности СПО.

Кроме приведенных выше частных рекомендаций по регулированию системных рисков существуют общие, универсальные меры, полезные для всех упоминавшихся рисков. Так, главный вывод по вопросу регулирования общесистемных рисков использования новых цифровых технологий заключается в том, что *новации будут полезны при большом объеме их*

---

[30] *Walshe P.* Digital Identities. 2020. P. 2. https://rm.coe.int/t-pd-2020-04rev-digital-identitytcen/1680a0c051 (дата обращения: 27.08.2025).

[31] Guidance on Digital ID // FATF. Paris. 06.03.2020. P. 87–88. https://www.fatf-gafi.org/en/publications/Financial inclusion and npoissues/Digital-identity-guidance.html (дата обращения: 31.08.2025).

[32] Principles on Identification for Sustainable Development: Toward the Digital Age (English). World Bank. Washington, D.C. 2022. P. 12. http://documents.worldbank.org/curated/en/213581486378184357/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age (дата обращения: 31.08.2025).

[33] Guidance on Digital ID // FATF. Paris, 06.03.2020. P. 6, 88. https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html (дата обращения: 31.08.2025).

[34] Principles on Identification for Sustainable Development: Toward the Digital Age (English). World Bank. Washington, D.C. 2022. P. 13. http://documents.worldbank.org/curated/en/213581486378184357/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age (дата обращения: 27.08.2025).

[35] Guidance on Digital ID // FATF. Paris, 06.03.2020. https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html (дата обращения: 27.08.2025).

[36] Principles on Identification for Sustainable Development: Toward the Digital Age (English). World Bank. Washington, D.C. 2022. http://documents.worldbank.org/curated/en/213581486378184357/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age (дата обращения: 27.08.2025).

[37] Возможности и проблемы новых технологий для ПОД/ФТ // ФАТФ. Париж, Франция, 2021. С. 48. https://www.fatf-gafi.org/content/dam/fatf-gafi/translations/guidance/Russian-Opportunities-and-Challenges-of-New-Technologies-for-AML-CFT.pdf (дата обращения: 27.08.2025).

внедрения в мире. Причем масштаб внедрения должен обеспечиваться путем использования нематериальных рычагов (введением нормативов обязательного внедрения и увеличением уровня доверительности между контролерами и контролируемыми субъектами)[38].

Для минимизации комплаенс-риска необходимо усиление контактов регуляторов и подконтрольных организаций и постоянный обмен информацией между ними («Компетентные органы должны предоставлять информацию и рекомендации по изменениям в нормативных актах…Постоянная координация между надзорными органами и другими государственными органами в их взаимодействии с частным сектором обеспечивает четкую передачу информации об ожиданиях в отношении управления рисками»[39]), путем изменения регуляторной политики и инструкций по эксплуатации ИТ («если предшествующая модель предполагала контроль от проверки к проверке, то новый ее формат … позволяет осуществлять постоянный мониторинг и комплексную оценку … деятельности организаций, но не столько в целях их наказания, сколько в целях их развития на основе своевременных рекомендаций и предупреждений» [6, с. 70]). Более подробная оценка рисков системы противодействия и меры их регулирования представлены в табл. 2.

По опросам ФАТФ обобщенная оценка важности условий внедрения новых технологий имеет следующий вид (в скобках указана доля респондентов (в %), отметивших данное условие в качестве ключевого для внедрения ИТ)[40]:

– благоприятный режим регулирования или стимулирования (79%);
– инвестиции в обеспечение конкурентоспособности (44%);
– подготовка специалистов, обладающих нужными компетенциями (41%);
– формирование спроса (30%);
– увеличение масштаба распространения ИТ (26%);
– ориентация государственных закупок на цифровые новации (24%).

Польза ИТ достигается при их масштабном внедрении, возможном при наличии требований об обязательном их использовании либо высоком доверии между регуляторами и регулируемыми субъектами. При этом необходим также интенсивный информационный обмен между подконтрольными организациями, между регулято-

[38] Там же. С. 63.

[39] Guidance for a Risk-Based Approach to the Real Estate Sector. FATF. Paris. July 2022. Pp. 11, 62. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/RBA-Real-Estate-Sector.pdf.coredownload.pdf (дата обращения: 31.08.2025).

[40] Возможности и проблемы новых технологий для ПОД/ФТ // ФАТФ. Париж, Франция, 2021. С. 49. https://www.fatf-gafi.org/content/dam/fatf-gafi/translations/guidance/Russian-Opportunities-and-Challenges-of-New-Technologies-for-AML-CFT.pdf (дата обращения: 30.08.2025).

Таблица 2

Оценка общесистемных рисков противодействия отмыванию денег и меры их регулирования

Факторы риска	Меры регулирования рисков
Риск: регулирование. Уровень риска 68%	
неспособность регулируемых субъектов отвечать за инновации; невозможность регуляторного надзора за ИТ; низкий уровень стандартизации; неуверенность в данных, обработанных ИТ; трудности в оценке толерантности к риску (*фактор эффективности*); сокращение времени выявления преступлений[а)] (*фактор скорости*); зависимость использования ИТ от регуляторов, а не технологий (*фактор избыточного регулирования*)	участие аккредитованных ИТ-компаний в обучении студентов ИТ-специальностей, разработка новых образовательных программ, привлечение преподавателей-практиков, обучение преподавателей и руководителей образовательных программ в сфере ИТ[б)]; использование реальных дел для машинного обучения вместо решений сотрудников; автоматизация обратной связи от контролеров; мониторинг эффективности регулируемых субъектов, обмен опытом и разработка руководств; демонстрация преимуществ ИТ для подконтрольных организаций[в)]
Риск: требования защиты данных и неприкосновенности личной жизни. Уровень риска 56%	
нарушения защиты данных	снижение «рисков непреднамеренной финансовой изоляции и нарушения правил неприкосновенности личной жизни» рассмотрено в Руководстве[г)]; принципы цифровой идентификации изложены в Принципах[д)]; мониторинг эффективности регулируемых субъектов, обмен опытом и разработка руководств
Риск: качество данных. Уровень риска 44%	
дисгармонизация данных; настройка новых систем и адаптация к среде; невозможность информационного обмена для подконтрольных организаций; трансляция ошибок ИИ; *фактор эффективности*; *фактор скорости*; *фактор избыточного регулирования*	оптимизация участия человека в проверке данных; обработка естественного языка для автоматизации ввода информации; мониторинг эффективности регулируемых субъектов, обмен опытом и разработка руководств

Продолжение табл. 2

Факторы риска	Меры регулирования рисков
Риск: технологии. Уровень риска 42%	
несоответствие надзорных стратегий ИТ; незнание разработчиками особенностей госзакупок; устаревание технологий; чрезмерные требования заказчика; трудность интеграции ИТ; отсутствие возможностей для ИТ; неудовлетворенность регуляторов возможностями ИТ (*фактор проверки*)	модернизация надзорных стратегий; мониторинг эффективности регулируемых субъектов, обмен опытом и разработка руководств
Риск: сложность ИТ. Уровень риска 39%	
несоответствие надзорных стратегий ИТ; сложность интеграции ИТ; отсутствие возможностей для ИТ; неготовность регуляторов к надзору за ИТ	модернизация надзорных стратегий; мониторинг эффективности регулируемых субъектов, обмен опытом и разработка руководств
Риск: стоимость ИТ. Уровень риска 37%	
высокая собственная стоимость ИТ; сложность интеграции; моральный износ ИТ; несогласованность информации; сложность закупки ИТ; *фактор эффективности*	мониторинг эффективности регулируемых субъектов, обмен опытом и разработка руководств
Риск: неприятие риска. Уровень риска 18%	
сложность оценки результативности малыми организациями (риск оценки); невыполнение требований противодействия; нарушение неприкосновенности личной жизни; информационные искажения при интеграции машинного обучения; транслирование ИИ ошибок; *фактор эффективности*; *фактор скорости*	развитие методологии регулирования риска; обработка естественного языка для автоматизации ввода информации; мониторинг эффективности регулируемых субъектов, обмен опытом и разработка руководств
Риск: отсутствие регулятивной песочницы для апробирования ИТ. Уровень риска 15%	
фактор проверки; *фактор эффективности*; *фактор скорости*	создание стандартного инструмента для испытаний ИТ; мониторинг эффективности регулируемых субъектов, обмен опытом и разработка руководств

Окончание табл. 2

Факторы риска	Меры регулирования рисков
Риск: коммерческие интересы. Уровень риска 13%	
нерезультативность ИТ; невозможность масштабирования технологий из-за дисгармонизации данных; *фактор эффективности*; *фактор скорости*	мониторинг эффективности регулируемых субъектов, обмен опытом и разработка руководств
Риск: угроза вмешательства со стороны преступников. Уровень риска 11%	
использование ИТ преступниками; влияние преступников на финансовые операции	мониторинг эффективности регулируемых субъектов, обмен опытом и разработка руководств
Риск: невозможность охвата всех слоев населения финансовыми услугами. Уровень риска 7%	
лишение финансовых услуг лиц с ограниченным доступом; *фактор скорости*	инклюзивность цифровой идентификации [е,ж,з]; гарантия достоверности идентификации на основе ИТ[и]; использование цифрового удостоверения личности[к]; устранение препятствий к доступу и использованию: устранение препятствий для реализации прав или доступа к основным услугам или льготам из-за расходов, устранение информационных барьеров и неравенства, устранение препятствий, связанных с отсутствием мобильного или интернет-соединения, электронных устройств, цифровых навыков, удобства или способности использования определенных технологий, уделение первоочередного внимания потребностям и проблемам маргинализированных и уязвимых групп[л]; использование принципов цифровой идентификации[м]; исключение чрезмерности опоры на ИТ; мониторинг эффективности регулируемых субъектов, обмен опытом и разработка руководств
Риск: нерезультативность сведений о подозрительных операциях (СПО). Уровень риска 3%	
недостатки в отправлении СПО; неэффективность СПО	использование личного кабинета для обратной связи по передаче СПО

а) Возможности и проблемы новых технологий для ПОД/ФТ. ФАТФ. Париж, Франция, 2021. С. 47. https://www.fatf-gafi.org/content/dam/fatf-gafi/translations/guidance/Russian-Opportunities-and-Challenges-of-New-Technologies-for-AML-CFT.pdf (дата обращения: 27.08.2025);
б) Минцифры. Кадры для цифровой трансформации. https://digital.gov.ru/activity/czifrovizacziya-gosudarstva/vedomstvennyj-proektnyj-ofis-vpo/administrirovanie-i-soprovozhdenie-ispolneniya-naczionalnogo-proekta-ekonomika-dannyh-i-czifrovaya-transformacziya-gosudarstva/cz8-kadry-dlya-czifrovoj-transformaczii (дата обращения: 27.08.2025);
в) *Coelho R., Simoni M.D. Prenio, J. BIS.* SupTech applications for AML // FSI Insights. August 2019. No 18. P. 1. https://www.bis.org/fsi/publ/insights18.pdf (дата обращения: 02.08.2024); Industry Perspectives – Adopting Data Analytics Methods for AML/CFT // A Singapore Government Agency Website. 12.11.2018. https://www.mas.gov.sg/regulation/external-publications/industry-perspectives-adopting-data-analytics-methods-for-amlcft (дата обращения: 31.08.2025);
г) Guidance on Digital ID. FATF. Paris, 06.03.2020. https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html (дата обращения: 28.08.2025);
д) Principles on Identification for Sustainable Development: Toward the Digital Age (English). World Bank. Washington, D.C. 2022. http://documents.worldbank.org/curated/en/213581486378184357/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age (дата обращения: 28.08.2025);
е) *Walshe P.* Digital Identities. 2020. P. 2. https://rm.coe.int/t-pd-2020-04rev-digital-identitytcen/1680a0c051 (дата обращения: 27.08.2025);
ж) Guidance on Digital ID // FATF. Paris, 06.03.2020. P. 87-88. https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html (дата обращения: 31.08.2025);
з) Principles on Identification for Sustainable Development: Toward the Digital Age (English). World Bank. Washington, D.C. 2022. P. 12. http://documents.worldbank.org/curated/en/213581486378184357/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age (дата обращения: 31.08.2025);
и) Guidance on Digital ID // FATF. Paris, 06.03.2020. Pp. 6, 88. https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html (дата обращения: 31.08.2025);
к) Там же;
л) Principles on Identification for Sustainable Development: Toward the Digital Age (English). World Bank. Washington, D.C. 2022. P. 13. http://documents.worldbank.org/curated/en/213581486378184357/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age (дата обращения: 31.08.2025);
м) Возможности и проблемы новых технологий для ПОД/ФТ. ФАТФ. Париж, Франция, 2021. С. 44. https://www.fatf-gafi.org/content/dam/fatf-gafi/translations/guidance/Russian-Opportunities-and-Challenges-of-New-Technologies-for-AML-CFT.pdf (дата обращения: 31.08.2025).

Источник: составлено автором по данным ФАТФ (Возможности и проблемы новых технологий для ПОД/ФТ // ФАТФ. Париж, Франция, 2021. https://www.fatf-gafi.org/content/dam/fatf-gafi/translations/guidance/Russian-Opportunities-and-Challenges-of-New-Technologies-for-AML-CFT.pdf (дата обращения: 30.08.2025).).

рами и подконтрольными организациями и адаптация регуляторной политики к меняющимся условиям среды функционирования.

Создавая благоприятный режим для распространения новаций, ФАТФ и надзорные органы не должны в то же время поддерживать определенные продукты или их разработчиков. Они должны содействовать инновациям с учетом государственных целей[41]. Но ответственность за противодействие лежит на регулируемых субъектах.

Заключение

Итак, проведенное исследование о внедрении информационных технологий с использованием опросов авторитетных организаций позволило идентифицировать факторы рисков и меры их регулирования, а также провести градацию системных рисков внедрения цифровых технологий для противодействия отмыванию денег (по уровню рисков). *Главным специальным системным рисковым фактором внедрения новаций является недостаточный уровень компетенций в сфере цифровых технологий ПОД* как у субъектов, деятельность которых регулируется, так и у регуляторов. Мерой воздействия на этот рисковый фактор, а также на факторы рисков качества данных, технологического риска и риска внедрения новых технологий является реализация политики подготовки кадров, включающей разработку специальных образовательных программ для студентов, преподавателей и сотрудников организаций, обеспечивающих ПОД, привлечение ИТ-компаний для обучения. С другой стороны, влияние данного фактора снизится, если регулятор гарантирует достаточное методическое обеспечение использования цифровых технологий, повысится уровень автоматизации отношений и обеспечится непрерывный обмен информацией между участниками противодействия.

Вторым по важности фактором риска является возможность нарушения защиты данных. Кроме интенсификации информационного обмена между всеми участниками ПОД мерой воздействия на данный фактор является повышение надежности технологий, рассматриваемой в контексте безопасности данных.

Для рисков некачественных данных, технологических рисков, рисков внедрения новых технологий и стоимости новых технологий кроме проблем с компетенциями субъектов, причастных к ПОД, в том числе и разработчиков программных продуктов, можно отметить такие факторы, как рассогласованность данных, получаемых из разных источ-

[41] Возможности и проблемы новых технологий для ПОД/ФТ // ФАТФ. Париж, Франция, 2021. С. 49. https://www.fatf-gafi.org/content/dam/fatf-gafi/translations/guidance/Russian-Opportunities-and-Challenges-of-New-Technologies-for-AML-CFT.pdf (дата обращения: 30.08.2025).

ников, несовместимость новых технологий со старыми, дороговизну их внедрения, неэффективность цифровых продуктов. Кроме реализации кадровой политики и снижения доли человеческого участия в процессах дополнительной мерой противодействия таким рисковым факторам является совершенствование надзорных стратегий.

Риск неприятия инновационных рисков связан с возможными ошибками в создании программных продуктов. Для малых и средних предприятий возникает еще проблема сложности формирования среды для работы с цифровыми технологиями. Для регулирования этих рисковых факторов кроме методологического обеспечения также можно предложить минимизацию участия людей в реализации процедур ПОД. Рисковый фактор оценки соответствия цифровых продуктов требованиям регуляторов может преодолеваться внедрением соответствующего инструментария тестирования новаций. Рисковые факторы неэффективности новаций и возможного преступного их использования связаны с масштабом распространения технологий. Снижение действия рискового фактора дискриминации каких-то лиц в получении ими финансовых услуг связано с возможностью более подробной идентификации клиентов путем анализа большого количества информации.

Наименее значимыми в списке важнейших факторов риска являются рисковые факторы передачи регулятору некачественной информации о подозрительных операциях. Противодействие таким факторам достигается путем внедрения личных кабинетов для участников ПОД.

Такое упорядочение рисковых факторов позволяет распределить ресурсы (финансовые, трудовые и пр.) воздействия на них в соответствии с оценками их важности и сосредоточить усилия прежде всего на противодействии важнейшим факторам. Тем самым появляется возможность для финансовых организаций предоставить услуги большему количеству экономических субъектов.

ЛИТЕРАТУРА / REFERENCES

1. *Козырев А.Н.* Цифровая экономика и экономика данных // Цифровая экономика. 2024. Т. 2. № 28. С. 5–14. [*Kozyrev A.N.* The Data Economy and the Digital Economy // Digital Economy. 2024. Vol. 2. No. 28. Pp. 5–14. (In Russ.).] DOI: 10.33276/DE-2024-02-01. EDN: BFNYBQ.
2. *Tapscott D.* The Digital Economy: Promise and Peril In The Age of Networked Intelligence: Monograph. New York, McGrawHill, 1995.
3. *Tapscott D.* The Digital Economy Anniversary Edition: Rethinking Promise and Peril In the Age of Networked Intelligence: Monograph. New York, McGraw-Hill, 2014.
4. *Coase R.* The Nature of the Firm // Econometrica. 1937. Vol. 4. No. 16. Pp. 386–405. DOI: 10.1111/j.1468-0335.1937.tb00002.x.
5. *Tapscott D., Agnew D.* Governance in the Digital Economy // Finance & Development. 1999. December. Pp. 34–37. https://www.imf.org/external/pubs/ft/fandd/1999/12/pdf/tapscott.pdf (accessed: 31.08.2025).

6. *Абасов И.Р., Галимханов А.Б., Юсупов Р.Г.* О контрольно-надзорной деятельности органов государственной власти Российской Федерации в сфере образования в условиях развития цифровых технологий // Правовое государство: теория и практика. 2023. Т.19. № 4 (74). С. 62–70. [*Abasov I.R., Galimkhanov A.B., Yusupov R.G.* On the monitoring and supervision of the state authorities of the Russian Federation in the field of education in the context of the digital technologies development // The Rule-of-Law State: Theory and Practice. 2023. No. 4. Pp. 62–70. (In Russ.).] DOI: 10.33184/pravgos-2023.4.7. EDN: SZURHB.

Дата поступления рукописи: *19.05.2025 г.*
Дата принятия к публикации: *13.10.2025 г.*

СВЕДЕНИЯ ОБ АВТОРЕ

Синявский Николай Григорьевич – доктор экономических наук, доцент, ведущий научный сотрудник Института экономической политики и проблем экономической безопасности Факультета экономики и бизнеса Финансового университета при Правительстве Российской Федерации, Москва, Россия
ORCID: 0000-0003-1034-6489
NSinyavskiy@fa.ru

ABOUT THE AUTHOR

Nikolai G. Sinyavsky – Dr. Sci. (Econ.), Associate Professor, Leading Researcher, Institute of Economic Policy and Economic Security Problems, Faculty of Economics and Business, Financial University under the Government of the Russian Federation, Moscow, Russia
ORCID: 0000-0003-1034-6489
NSinyavskiy@fa.ru

SYSTEMIC RISK FACTORS IN THE IMPLEMENTATION OF DIGITAL TECHNOLOGIES TO ANTI-MONEY LAUNDERING: IDENTIFICATION, RANKING AND REGULATORY MEASURES

Digital products have the potential to make anti-money laundering and counter-terrorist financing operations less costly, more efficient and significantly faster, ensure high-quality compliance with the Financial Action Task Force Standards and improve cross-border cooperation. This enables financial institutions to provide services to a greater number of economic entities. Therefore, the global anti-money laundering system is widely introducing innovative digital technologies to provide prompt and reliable information about economic entities and their operations by significantly increasing the volume of processed data. However, their use is associated with regulatory or operational systemic risks. The purpose of the study is to identify risk factors and measures to regulate them for systemic risks, as well as to systematize and rank them by importance. Such ordering provides grounds for the appropriate distribution of resources used to influence risk factors. The level of risks, risk factors and measures for their regulation are assessed on the basis of a risk-oriented approach using surveys of authoritative organizations, research by specialists and regulatory documents.

Keywords: *anti-money laundering, Financial Action Task Force on Money Laundering (FATF), digitalization, risks.*
JEL: O33, O38, L73.