РИСКИ ИСПОЛЬЗОВАНИЯ ФИНАНСОВЫХ ТЕХНОЛОГИЙ В СХЕМАХ ПОД\ФТ. ТИПОЛОГИИ И ПРОГНОЗ

Костеева Ирина Сергеевна

студент, Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, Липецкий филиал, РФ, г. Липецк

Кривых Николай Николаевич

научный руководитель, канд. экон. наук, Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, Липецкий филиал, РФ, г. Липецк

Аннотация. В статье рассматриваются ключевые риски, связанные с использованием новых финансовых технологий (финтеха) в противоправных схемах, направленных на отмывание доходов, полученных преступным путём, и финансирование терроризма (ПОД/ФТ). Особое внимание уделяется типовым механизмам, включая использование криптовалют, децентрализованных финансов (DeFi), цифровых кошельков, а также технологий токенизации и микротранзакций.

Ключевые слова: финансовые технологии; ПОД/ФТ; криптовалюта; DeFi; отмывание доходов; финансирование терроризма; цифровая идентификация; финтех; риски; прогноз.

Современное развитие финансовых технологий (финтех) оказывает значительное влияние на трансформацию глобальной финансовой системы, обеспечивая удобство, доступность и скорость проведения операций. Однако наряду с очевидными преимуществами внедрение цифровых инструментов, включая криптовалюты, децентрализованные финансовые платформы (DeFi), токенизированные активы и алгоритмические механизмы расчётов, приводит к возникновению новых рисков в сфере противодействия отмыванию доходов, полученных преступным путём, и финансированию терроризма (ПОД/ФТ).

Актуальность проблемы обусловлена стремительным расширением использования финтех-решений как в легальном секторе, так и в теневой экономике. Новые технологии зачастую опережают по темпам развития механизмы нормативно-правового регулирования и надзора, что создаёт благоприятную среду для использования этих инструментов в незаконных целях. Согласно данным Межправительственной группы разработки финансовых мер борьбы с отмыванием денег (FATF), децентрализованные платформы и анонимные криптовалютные транзакции всё чаще используются для маскировки происхождения средств и трансграничных переводов с целью финансирования экстремистской деятельности.

В текущих условиях глобальной цифровизации особое значение приобретает разработка эффективных методов мониторинга и анализа новых угроз, связанных с использованием финансовых технологий. Несмотря на предпринимаемые международным сообществом меры, включая обновление стандартов FATF, внедрение принципов Know Your Customer (KYC) и усиление межгосударственного обмена информацией, наблюдается рост числа схем, основанных на цифровой анонимности, технологической сложности и юрисдикционной фрагментации.

Одним из ключевых вызовов, стоящих перед системой ПОД/ФТ сегодня, является использование новых финансовых технологий, которые предоставляют пользователям практически неограниченные возможности в части скорости, масштабируемости и анонимности транзакций. В отличие от традиционных банковских систем, финтех-продукты зачастую функционируют вне рамок классического регулирования, что делает их привлекательными для злоумышленников.

Во-первых, особую обеспокоенность вызывает анонимность транзакций. Многие криптовалюты, в том числе так называемые "privacy coins" (например, Monero или Zcash), изначально были спроектированы с акцентом на приватность и отсутствие возможности отслеживания отправителя или получателя. Даже в случае с популярными активами, такими как Bitcoin, существуют сервисы микширования (mixers, tumblers), позволяющие размыть цепочку следов, затрудняя расследование и финансовый мониторинг.

Во-вторых, распространение децентрализованных финансовых платформ (DeFi), функционирующих на базе смарт-контрактов, создало совершенно новое пространство для операций, которые осуществляются без участия центрального контрагента. Такие платформы не требуют прохождения процедуры идентификации (KYC), а все действия выполняются автоматически через код. Это открывает возможности для обхода финансового регулирования, а в некоторых случаях — и для финансирования противоправной деятельности.

В-третьих, существенные риски связаны с отсутствием глобально унифицированного регулирования. Многие проекты финтеха зарегистрированы в юрисдикциях с мягким комплаенсом или вовсе функционируют без формальной регистрации. Такая среда становится питательной почвой для развития серых и теневых схем, направленных на легализацию доходов, полученных преступным путём.

В-четвёртых, проблема недостаточного уровня цифровой грамотности как со стороны пользователей, так и со стороны контролирующих органов, усиливает уязвимость к мошенническим действиям. Преступные группы нередко используют подставные лица, поддельные документы или взломанные аккаунты для создания фиктивных цифровых кошельков, из которых затем осуществляются переводы и конвертация средств в менее отслеживаемые активы.

С учётом текущих трендов в цифровизации финансовых рынков, можно с высокой долей уверенности утверждать, что в ближайшие годы характер угроз в сфере ПОД/ФТ претерпит качественные изменения. Технологии становятся не только инструментом развития, но и фактором уязвимости, особенно в условиях, когда регулирование не успевает за инновациями. Наиболее очевидная тенденция — активное внедрение ИИ в процессы отмывания средств. Уже сейчас можно наблюдать использование ИИ-алгоритмов для автоматизации переводов, создания фальшивых профилей с правдоподобной историей транзакций, а также генерации документов, подделать которые ранее было крайне затруднительно. Генеративные модели, в том числе deepfake-технологии, могут быть применены для обхода систем биометрической идентификации, что открывает новые горизонты для мошеннических операций.
С переходом части цифровой активности в метавселенные и Web3-инфраструктуры, появляются платформы, в которых пользователи могут владеть и передавать активы в виде токенов, в том числе NFT, с минимальным уровнем контроля. Эти активы, зачастую слабо привязанные к фиатной валюте, могут служить средством перемещения ценностей между юрисдикциями, оставаясь за пределами поля зрения финансового мониторинга.

Финансовые технологии становятся всё более децентрализованными и международными. Один пользователь может находиться в Юго-Восточной Азии, другой — в Восточной Европе, а сама платформа — быть зарегистрирована в оффшорной зоне. Это создаёт серьёзные препятствия для надзора и раскрытия информации о конечных бенефициарах. Если раньше правоохранительные органы могли опереться на банковские каналы для получения данных, то теперь взаимодействие с DeFi-платформами требует иных подходов и международной координации. Киберпреступность становится всё более специализированной. Угрозу представляют не только незаконные транзакции, но и компрометация целых платформ: взломы кошельков, перехват смарт-контрактов, «дренаж» ликвидности из DeFi-протоколов.

Это не только наносит ущерб пользователям, но и даёт преступникам доступ к крупным объёмам цифровых активов, которые затем могут быть интегрированы в преступные схемы.

Прогнозируется, что государства будут вынуждены ускорить разработку нормативных актов, касающихся регулирования финтеха. При этом будет сохраняться конфликт между интересами инновационного бизнеса и требованиями национальной и международной безопасности. Возможно появление новых стандартов финансового мониторинга, интегрированных в блокчейн-экосистемы, а также развитие механизмов цифровой сертификации участников.

В результате, прогнозируемый вектор развития угроз в сфере ПОД/ФТ связан с технологическим усложнением схем и расширением зон юридической неопределённости. Эффективная реакция со стороны государства и международного сообщества требует не только ужесточения контроля, но и внедрения инновационных решений на уровне самих надзорных систем — от интеллектуального анализа транзакций до интеграции цифровых паспортов и блокчейн-идентификаторов.

Использование новых финансовых технологий создаёт не только возможности для ускорения и оптимизации финансовых процессов, но и представляет серьёзные вызовы для систем ПОД/ФТ. Рост анонимных и децентрализованных инструментов, использование ИИ, переход в Web3 и слабость международного регулирования формируют благоприятную среду для развития преступных схем. В этих условиях особенно важно обеспечить баланс между стимулированием инноваций и надёжной системой контроля. Эффективное противодействие новым угрозам требует как адаптации нормативно-правовой базы, так и активного международного сотрудничества.

Список литературы:

1. Beosin. 2024 Q3 Global Web3 Security Report, AML Analysis & Crypto Regulatory Landscape [Электронный ресурс]. URL: https://beosin.com/resources/2024_Q3_Global_Web3_Security_Report%2C_AML_Analysis_%26_Crypto_Regulatory_Landscape_.pdf (дата обращения: 03.04.2025).

2. Cambridge Centre for Alternative Finance. 2nd Global Cryptoasset Regulatory Landscape Study [Электронный ресурс]. Октябрь 2024 г. URL: https://www.jbs.cam.ac.uk/wp-content/uploads/2024/10/2024-2nd-global-cryptoasset-regulatory-landscape-study.pdf (дата обращения: 03.04.2025).

3. Chainalysis. 2024 Crypto Money Laundering Report [Электронный ресурс]. URL: https://www.chainalysis.com/blog/2024-crypto-money-laundering/ (дата обращения: 03.04.2025).

4. Egmont Group. Report on Abuse of Virtual Assets for Terrorist Financing Purposes [Электронный ресурс]. Июль 2023 г. URL: https://egmontgroup.org/wp-content/uploads/2023/12/2023-July-HoFIU-06-IEWG-Project-Abuse-of-VA-for-TF-Summary-1.pdf (дата обращения: 03.04.2025).

5. Financial Action Task Force (FATF). 12-Month Review of Revised FATF Standards – Virtual Assets and VASPs [Электронный ресурс]. URL: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/12-month-review-virtual-assets-vasps.html (дата обращения: 03.04.2025).