УДК 336:343.301
DOI 10.26118/7121.2026.32.25.010

Малюгина Мария Дмитриевна
Финансовый университет при Правительстве Российской Федерации
Сергеева Виолетта Сергеевна
Финансовый университет при Правительстве Российской Федерации
Чернышова Елена Николаевна
Финансовый университет при Правительстве Российской Федерации

Тёмная сторона цифровизации: использование новых технологий для отмывания денег и финансирования терроризма

Аннотация. В статье исследуется проблема нелегальных транзакций с использованием цифровых активов в целях выявления ключевых угроз «тёмной стороны» цифровизации в контексте отмывания денег (AML) и финансирования терроризма (CFT). Представлена комплексная типология цифровых схем отмывания денег и финансирования терроризма, проведен анализ новых форм противоправных действий, определены ключевые уровни уязвимостей. Встроенная трансграничность, относительная анонимность и трудности правового регулирования ведут к масштабному использованию цифровых технологий в отмывании денег и финансировании терроризма. В целях эффективного, опережающего противодействия необходимо развитие законодательства в сфере ПОД/ФТ, внедрение передовых инструментов аналитики (блокчейн-форензика для автоматического выявления аномалий и связей в финансовых потоках), постоянный мониторинг новых технологических трендов (DeFi 2.0, метавселенные, AI-трейдинг).

Ключевые слова: цифровизация, отмывание денег, финансирование терроризма, криптовалюты, децентрализованные финансы, финансовые технологии, AML/CFT

Malyugina Maria Dmitrievna
Financial University under the Government of the Russian Federation
Sergeeva Violetta Sergeevna
Financial University under the Government of the Russian Federation
Chernyshova Elena Nikolaevna
Financial University under the Government of the Russian Federation

The dark side of digitalization: using new technologies for money laundering and terrorist financing

Abstract. This article examines the problem of illegal transactions using digital assets to identify key threats posed by the "dark side" of digitalization in the context of anti-money laundering (AML) and counter-terrorist financing (CFT). A comprehensive typology of digital money laundering and counter-terrorist financing schemes is presented, new forms of illegal activity are analyzed, and key vulnerabilities are identified. The inherent cross-border nature, relative anonymity, and regulatory challenges are leading to the widespread use of digital technologies in money laundering and counter-terrorist financing. Effective, proactive countermeasures require the development of AML/CFT legislation, the implementation of advanced analytical tools (blockchain forensics for the automatic detection of anomalies and connections in financial flows), and ongoing monitoring of emerging technological trends (DeFi 2.0, metaverses, AI trading).

Keywords: digitalization, money laundering, terrorist financing, cryptocurrency, decentralized finance, financial technology, AML/CFT

Актуальность. Цифровизация экономики и финансовых услуг создаёт не только новые возможности для добросовестных участников рынка, но и формирует «тёмную сторону» – цифровые пространства, где злоумышленники могут легче скрывать незаконные операции. Международные институты фиксируют устойчивый рост таких эпизодов: только в 2023 г. объём средств, переведённых на адреса, связанные с незаконной активностью, превысил $24 млрд, что иллюстрирует масштаб вызова для финансовой стабильности и нацбезопасности. Вольфганг Хетцер еще в 2002 году в своей статье «Отмывание денег посредством электроники» пророчески писал: «анонимный и виртуальный мир банковских операций «онлайн» может стать эльдорадо для лиц, занимающихся отмыванием денег» [19].

Появление криптовалют, теневых онлайн-казино, NFT-платформ и прочих финтех-новшеств существенно усложнило контроль финансовых потоков. Электронные сети и телекоммуникации позволяют проводить сделки практически бесконтрольно, создавая огромный криминогенный потенциал для легализации преступных доходов. В этих условиях актуальность темы крайне высока: нелегальные транзакции в цифровой среде угрожают финансовой стабильности и национальной безопасности.

Изученность проблемы. Противодействие отмыванию денег и финансированию терроризма в условиях цифровой экономики – предмет исследований как международных организаций, так и ученых в области финансов, права и кибербезопасности. Регулярно публикуются доклады, оценивающие новые угрозы: так, ФАТФ выпустила специализированные руководства по виртуальным активам и сервисам, подчёркивая необходимость глобального регулирования, чтобы криптоактивы не стали укрытием для преступников и террористов. Chainalysis и другие аналитические компании ежегодно отслеживают тренды киберпреступности, фиксируя, например, рост доли стейблкоинов в нелегальных транзакциях и активность санкционированных игроков. В научной литературе рассматриваются методы «электронного» отмывания денег, схемы обхода мер комплаенса, вопросы юрисдикционного арбитража. Вместе с тем, ввиду новизны многих технологий и их быстрой эволюции, ряд аспектов изучен недостаточно – особенно касательно риск-ориентированных подходов к ним и влияния регуляторных нововведений последних лет. В этой связи необходимо комплексное исследование, объединяющее технологические, правовые и финансовые аспекты проблемы.

Цель работы – выявление ключевых угроз, связанных с использованием современных цифровых технологий для отмывания денег и финансирования терроризма, а также определение направлений совершенствования механизмов противодействия данным противоправным практикам.

Методология исследования заключается в применении системного подхода и междисциплинарного анализа. Применены общенаучные методы: анализ и синтез – для изучения отдельных элементов (технологий, правовых норм) и их синтеза в общую картину угроз; сравнение – для сопоставления национальных и международных практик регулирования; обобщение и абстрагирование – при формулировании выводов и предложений. В качестве специальных методов использованы ретроспективный анализ (для рассмотрения эволюции подходов к ПОД/ФТ с появлением новых технологий) и кейсовый метод (разбор конкретных инцидентов и схем). Информационной базой послужили открытые данные правоохранительных органов (МВД, ФСБ, Минюста), материалы международных организаций (FATF, ООН, Basel Institute), отчеты аналитических компаний (Chainalysis, CipherTrace), а также научные публикации по тематике противодействия финансовым преступлениям. Надёжность результатов обеспечена привлечением большого числа источников и их критическим анализом, что позволяет учесть различную природу угроз.

Эмпирическую основу исследования составили случаи, зафиксированные в 2018-2024 гг. в различных странах, демонстрирующие использование цифровых инструментов для противоправных целей. Синтез разнообразных источников позволил сформировать целостное представление о проблеме и разработать аргументированные рекомендации.

Теоретическая значимость заключается в систематизации и обобщении представлений об угрозах, которые возникают при использовании современных цифровых технологий в финансовом секторе. Анализ показал, что новые инструменты расширяют каналы легализации преступных доходов, обеспечивая анонимность и высокую скорость трансграничных транзакций. Такие свойства цифровых финансов значительно усложняют выявление схем отмывания денег и финансирования терроризма, что сопряжено с возрастающими рисками для глобальной финансовой стабильности, национальной и международной безопасности.

Научная новизна обусловлена разработкой комплексной типологии цифровых схем отмывания денег и финансирования терроризма и анализом новых форм их реализации. В работе выделены ключевые уровни уязвимостей: криптовалютные и анонимные сервисы, децентрализованные финансы и альтернативные цифровые активы; показано также использование онлайн-краудфандинга для сбора средств преступного происхождения. На основе проведённой типологии сформулированы выводы о рисках для глобальной финансовой стабильности и национальной безопасности, а также обоснована необходимость нормативно-правовой адаптации для минимизации этих рисков.

Основная часть

Результаты. Трехэтапная модель и её цифровое измерение. Классическая схема отмывания денег традиционно включает три стадии: размещение (placement), расслоение (layering) и интеграция (integration). Цифровые технологии влияют на каждую из них, особенно усложняя вторую и третью стадии. На этапе размещения преступники стараются ввести наличные средства в финансовую систему – с развитием финансовых технологий это всё чаще происходит через мобильные платежные сервисы, онлайн-кошельки, покупку криптовалют за наличные. Парадоксально, но именно этап физического ввода денег остаётся самым уязвимым – крупные суммы наличности относительно легко отследить при пересечении границ или внесении на счета.

Далее, на этапе расслоения незаконные доходы отрываются от источников посредством серии сложных транзакций: цифровые платформы позволяют создать запутанные цепочки переводов через десятки счетов, миксеры, обменники и различные токены. Если преступнику удалось успешно разместить средства, то последующее их «раздробление» в киберпространстве затрудняет работу правоохранителей – операции наслаиваются друг на друга, скрывая происхождение денег.

Наконец, на этапе интеграции отмытые активы возвращаются в экономику под видом легитимных – например, вложений в бизнес, недвижимости или ценные цифровые объекты. Если предыдущие стадии были пройдены успешно, отделить “очищенные” средства от законных практически невозможно без спецопераций.

Верховный Суд Российской Федерации подчеркивает, что для наличия состава преступления, предусмотренного статьей 174.1 УК (отмывание денежных средств, полученных преступным путем), не требуется обязательного вовлечения легализуемых денежных средств в экономический оборот, поскольку ответственность по указанной статье закона наступает при установлении самого факта совершения финансовых операций с целью придания правомерного вида владению. Это важное юридическое разъяснение, учитывающее специфику криптовалют: даже простое конвертирование криптоактивов в фиат и распределение по счетам признаётся отмыванием, если имело цель скрыть источник.

Типология цифровых инструментов, используемых злоумышленниками. Проведенное исследование позволило выделить три уровня цифровых технологий, задействованных в современных схемах отмывания денег и финансирования терроризма.

Первый уровень – криптовалюты и анонимные сервисы. Классические криптовалюты (Bitcoin, Ethereum и др.) и сопутствующие сервисы (миксеры, tumblers) являются базовым инструментом преступников. Криптовалюта представляет собой децентрализованную систему расчетов без участия банков, что обеспечивает псевдо-анонимность транзакций. За последние пять лет на криптобиржи было отправлено около $100 млрд «грязной» криптовалюты, связанной с незаконной деятельностью. Пример – организация

финансирования терроризма в Томской области (2020–2023): организатор канала использовал криптовалютный кошелек, чтобы регулярно передавать средства международной террористической организации для приобретения вооружения, транспортных средств, амуниции и пропаганды террористической деятельности (возбуждено уголовное дело по признакам состава преступления, предусмотренного ч. 4 ст. 205.1 УК РФ) [11].

Особую роль играют криптомиксеры – онлайн-сервисы, смешивающие криптовалютные транзакции множества пользователей для сокрытия цепочки происхождения монет. По сути, они дробят и объединяют средства разных клиентов, возвращая каждому эквивалентную сумму с новых адресов, разорвав связь с исходным кошельком. Это критический элемент схем: именно на этапе расслоения злоумышленники стремятся максимально запутать отслеживание. Из-за миксеров установить бенефициаров становится почти нереально – связь средств с первоисточником практически теряется. В данном случае примером является Tornado Cash – децентрализованный эфириум-миксер, позволявший анонимизировать транзакции без посредников. В августе 2022 г. Управление по контролю за иностранными активами (OFAC) Министерства финансов США внесло Tornado Cash в санкционный список, указав на его роль в отмывании ~$455 млн для северокорейской хакерской группировки Lazarus [9]. Однако в ноябре 2024 г. федеральный апелляционный суд США постановил, что санкции против смарт-контрактов Tornado Cash были незаконны. В марте 2025 г. OFAC сняло санкции, хотя уголовное преследование организаторов сервиса продолжается [15]. Этот случай подчеркивает сложность правовой оценки децентрализованных инструментов: с одной стороны, они объективно используются для преступных целей, с другой – их децентрализация бросает вызов традиционным механизмам санкций и контроля.

Другой пример – биткойн-миксер Blender.io, против которого США также ввели санкции в мае 2022 г., обвинив в содействии северокорейским хакерам: через Blender были обработаны не менее $20,5 млн из украденных ~$620 млн в проекте Axie Infinity [14]. Таким образом, в ответ на первый уровень угроз регуляторы применяют новые меры – санкции против криптосервисов, развитие аналитических инструментов. Но преступники продолжают активно использовать криптовалюты благодаря их глобальному характеру и недостатку унифицированного надзора.

Преступники также используют краудфандинговые платформы. Так, гражданин Канады Халилуллах Юсуф в 2021–2023 гг. создал несколько кампаний на краудфандинговых платформах под видом благотворительности, собрав десятки тысяч долларов. Средства поступали от множества мелких доноров по всему миру в криптовалюте, после чего он с сообщниками конвертировал часть пожертвований в биткоины и перевел на кошельки боевиков, а также использовал иных платежных посредников. Его сеть раскрыта усилиями RCMP и ФБР. Этот случай продемонстрировал, как краудфандинг и массовые цифровые платформы могут быть эксплуатированы для террористических целей: мельчайшие суммы от множества людей трудно отследить и связать с террористической сетью без международного обмена данными [18].

Второй уровень – децентрализованные финансовые платформы. DeFi представляет собой экосистему приложений на блокчейне, позволяющих проводить финансовые операции (кредиты, обмен, инвестирование) без посредников и вне прямого контроля регуляторов. Злоумышленники освоили DeFi-протоколы для усложнения отслеживания активов. Одним из случаев использования DeFi платформ для отмывания денег, стал инцидент с взломанной атакой на биржу криптовалют KuCoin в сентябре 2020 года – хакеры похитили криптоактивы на сумму более $150 млн и затем через децентрализованные биржи стали дробить и конвертировать средства. Аналитики отмечают, что даже легитимные средства, прошедшие через DeFi, могут получить средний уровень риска из-за потенциального смешения с грязными активами. Преступники также используют кросс-чейн технологии – перевод средств между разными блокчейнами через мосты (bridge-протоколы), что фрагментирует цепочку и требует от следователей владения данными по множеству сетей.

Децентрализация и анонимность таких платформ создают системный вызов для борьбы с отмыванием денег (AML, Anti-Money Laundering), ведь традиционные механизмы здесь неприменимы. Международные регуляторы только начинают вырабатывать подходы: так, FATF требует распространить правила «travel rule» (регуляторный стандарт, который обязывает поставщиков услуг виртуальных активов, таких как криптобиржи и кошельки, обмениваться информацией об отправителях и получателях при криптовалютных переводах) и на децентрализованные платформы.

ЕС в рамках регуляции MiCA (всеобъемлющий регламент для регулирования криптовалют, стейблкоинов и поставщиков крипто-услуг, введенный для защиты потребителей, обеспечения финансовой стабильности и прозрачности рынка, устанавливающий единые правила для выпуска токенов, лицензирования крипто-бирж и кошельков, а также требований к капиталу для компаний) тоже пытается охватить некоторые DeFi-активности. Тем не менее, воплощение этих норм затруднено – DeFi-протоколы могут разворачиваться автономно, без юридического лица. Следовательно, на втором уровне противодействие сводится пока что к аналитике и техническому мониторингу: отслеживанию подозрительных моделей движения средств, маркировке адресов с высоким риском и развитию средств блокчейн-аналитики, интегрируемых в национальные системы финансового мониторинга.

Третий уровень – альтернативные цифровые активы. К самым новым инструментам относятся невзаимозаменяемые токены (NFT) и объекты из онлайн-игр, которые начали применяться для скрытой передачи стоимости. NFT – это уникальные токены, подтверждающие право на цифровой объект (картинку, видео, игровой артефакт). Их привлекательность для мошенников связана с двумя факторами: пониженная прозрачность владельца и субъективная ценность актива (NFT «стоит столько, сколько за него заплатят»). Злоумышленник может провести схему «wash trading» – создать собственный NFT и многократно продать его самому себе через подставные аккаунты, постепенно увеличивая цену. В результате образуется запись о серии продаж актива по высоким ценам, и впоследствии NFT продаётся независимому покупателю, которому деньги от криминальной деятельности выдаются под видом оплаты за «коллекционный» токен. Так происходит отмывание: преступник получает легальное обоснование средств в виде продажи цифрового искусства, при этом истинный источник дохода скрыт. NFT-трейдинг не знает границ и таможен, сделки могут совершаться анонимно по всему миру, а отсутствие чётких правил оценки позволяет манипулировать ценой.

Ещё одна сфера – онлайн-игры. Например, внутренняя валюта в таких развлечениях может покупаться за «грязные» деньги, а затем перепродаваться за фиат добросовестным игрокам, что формально выглядит как игровая торговля [12].

Обобщая результаты, следует заключить, что цифровые технологии расширили арсенал преступников, позволив им увеличивать скорость, объём и географический размах незаконных транзакций, многократно усложнять отслеживание денежных потоков за счёт инновационных схем и использовать новые прикрытия для легализации доходов. К 2024 г. структура нелегальных операций претерпела изменения: если ранее доминировали прямые мошенничества и торговля запрещенными веществами, то сейчас значительную долю составляют нарушения санкций и киберпреступления, а также “вторичная” легализация похищенных и коррупционных средств. Преступная деятельность идет в ногу с технологическим развитием и вместе с тем, государственный контроль также совершенствуется, для снижения общего объёма незаконных криптоопераций. Тем не менее, риски остаются высокими, и необходимо понимание этих результатов для выработки адекватных мер реагирования.

Обсуждение. На основе результатов исследования можно выделить ряд ключевых рисков, возникающих на стыке цифровизации и противодействия финансовым преступлениям:

1) Скорость и глобальный масштаб транзакций. Цифровые платежные сервисы позволяют переводить огромные суммы почти мгновенно и через границы. Peer-to-peer сети, криптобиржи, онлайн-банкинг работают круглосуточно, что лишает органы контроля времени для обнаружения подозрительной активности. Кроме того, глобальность означает, что преступники могут легко перебрасывать средства в юрисдикции с более мягким контролем. Это создает эффект «перелива воды»: при ужесточении режима в одной стране, нелегальные операции мигрируют в другую. Например, после закрытия крупнейшего даркнет-маркетплейса Hydra в 2022 г. значительная часть торговцев переключилась на иностранные площадки, а объём торговли на darknet в 2023 г. вновь вырос. Риск заключается в том, что ни одна страна в одиночку не может эффективно блокировать глобальные нелегальные потоки – требуется согласованные международные действия.

2) Новые способы обхода идентификации и контроля. Несмотря на внедрение принципов KYC/AML большинством легальных финансовых организаций, злоумышленники находят пути обойти идентификацию. Используются обменники без лицензии, p2p-рынки, OTC-брокеры, которые готовы обменять наличные на криптовалюту без проверки документов. Распространена практика оформления счетов на подставных или украденных лиц – так называемые «дропперы», которые за плату предоставляют свои банковские аккаунты для транзита средств. Цифровые технологии, такие как Deepfake и сим-фермы, позволяют даже пройти поверхностные видео-KYC проверки, выдавая мошенника за другого человека. В итоге получается «низкая цифровая зрелость» некоторых субъектов: многие мелкие финансовые компании или региональные банки не имеют достаточных ресурсов для глубокого мониторинга, а преступники этим пользуются. Риск также связан с появлением новых платёжных продуктов, которые выпускаются финтех-стартапами с менее строгим комплаенсом. Эти уязвимости активно задействуются для дробления сумм ниже порога контроля и для «структурирования» транзакций.

3) Технологические барьеры для регуляторов. Государственным органам зачастую не хватает современных инструментов и экспертизы, чтобы противостоять высокотехнологичным схемам. Возникает проблема непрозрачности алгоритмов: когда банки внедряют системы искусственного интеллекта для мониторинга, сами регуляторы не всегда могут проверить, как эти «чёрные ящики» принимают решения. С другой стороны, преступники тоже используют шифрование, анонимные сети (TOR, I2P), mixing-сервисы для коммуникаций, что усложняет оперативную работу. Подчеркнем и риски кибербезопасности: взломы финансовых платформ приводят к крупным хищениям, как в случае с Ronin/Axie Infinity, и эти средства затем идут на финансирование незаконных программ. Регуляторы вынуждены не только ловить отмывателей, но и реагировать на новые атаки – это двойная нагрузка на их ИТ-инфраструктуру.

4) Конфиденциальность и безопасность. Цифровая трансформация финансов затрагивает права граждан, связанные с конфиденциальностью данных. Расширенный обмен информацией между банками и государством улучшает выявление преступлений, но несёт риск для защиты персональных данных. Страны стараются найти баланс – вводят ограничения на использование анонимных инструментов, но получают критику со стороны общества (опасения, что цифровой профайл каждого человека будет тотально отслеживаться). Пример – дискуссия о CBDC (цифровых валютах центральных банков): США в 2023-2024 гг. рассматривали Anti-CBDC Act, запрещающий ФРС выпускать цифровой доллар из опасений тотального финансового надзора. И хотя этот вопрос напрямую не касается отмывания, он отражает общую проблему: усиление мониторинга должно сопровождаться гарантиями от злоупотреблений и утечек данных. Иначе возрастает риск «непреднамеренных последствий» – например, исключения добропорядочных клиентов из системы из-за слишком жёстких фильтров, или препятствий финансовой инклюзии для уязвимых групп.

5) Трансграничные и юрисдикционные вызовы. Финансовые преступления в цифровой среде не признают государственных границ. Это требует беспрецедентного международного сотрудничества, стандартизации подходов и обмена информацией в режиме реального

времени. Пока что этого достичь трудно: разные страны находятся на разном уровне готовности. Одни (как США, Сингапур, Швейцария) активно внедряют регулирование криптовалют и аналитические системы, другие отстают или вообще запрещают обращение криптоактивов, что смещает проблему в «тени». FATF еще в 2018-2019 гг. обновила свои «Рекомендации», включив правило путешественника (Travel Rule) для криптовалют – требование передавать данные отправителя и получателя при переводах. Однако не все страны полностью реализовали эти стандарты. Ландшафт остаётся неоднородным: различные требования KYC к криптобиржам, отсутствие единого черного списка подозрительных кошельков, нестыковки в процедурах экстрадиции киберпреступников. В результате преступники легко выбирают наиболее «удобную» юрисдикцию для оперирования – например, регистрируют обменники в офшорах, хранят сервера в странах с низким уровнем киберкриминализации и прочее.

Возросшие угрозы требуют совершенствования мер противодействия и развития регулированияв данной сфере, в том числе на международном уровне. Анализ опыта разных стран показывает, что наибольшего успеха добиваются комплексные меры, сочетающие обновление законодательства, технологические решения и институциональные реформы.

Многие государства приняли или готовят законы, признающие цифровые активы и устанавливающие правила их оборота. В России основным актом является закон от 7 августа 2001 г. №115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», а в целях соблюдения рекомендаций ФАТФ в стране был принят Федеральный закон №259-ФЗ «О цифровых финансовых активах, цифровой валюте и внесении изменений в отдельные законодательные акты Российской Федерации» от 31.07.2020 г. На законодательном уровне закрепили понятие цифрового финансового актива, а также требования к деятельности операторов информационной сети, принятию решения о выпуске, учету и обращению цифровых активов. На международном уровне: принят регламент MiCA, вводящий лицензирование криптообменников и эмитентов стейблкоинов в рамках ЕС. Также летом 2025 г. в Европе начало работу Европейское антимонопольное агентство (AMLA) – орган, который планирует с 2028 г. напрямую взять под надзор до 40 крупнейших финансовых организаций. В США летом 2025 г. одобрили пакет законов («Clarity Act», «Genius Act», «Anti-CBDC Surveillance State Act»), направленных на разграничение юрисдикции между SEC и CFTC по контролю криптоактивов, регулирование стейблкоинов (требование резервного обеспечения 1:1) и ограничение для ФРС выпуска цифрового доллара [13, 2]. Таким образом, прослеживается тренд - цифровые активы перестают быть вне законов и включаются в периметр финансового регулирования, что является необходимым условием для дальнейшей борьбы с их криминальным использованием.

Силовые структуры и финмониторинг во многих странах внедряют специализированные ИТ-платформы для анализа криптотранзакций и больших данных. В России с 2021 г. функционирует разработанная Росфинмониторингом система «Прозрачный блокчейн» – централизованная платформа, которая позволяет отслеживать операции с криптовалютами путём процедуры KYC. За это время к системе подключились более 12 тыс. сотрудников правоохранительных органов и международных антиотмывочных служб, её уже начали тестировать банки (к концу 2025 планировалось массовое подключение банковского сектора). По данным Росфинмониторинга, только за 2024 г. с помощью «Прозрачного блокчейна» выявлено на 47% больше подозрительных операций с цифровыми активами, чем годом ранее [16].

Кроме того, в августе 2024 стало известно о выделении ~10,61 млрд руб. до 2030 г. на создание Единой информационной системы противодействия отмыванию денег в рамках национальной программы «Цифровая экономика» [4]. Эта платформа будет мониторить криптовалютные транзакции с целью деанонимизации владельцев цифровых кошельков, интегрирует пять федеральных органов исполнительной власти, применяет ИИ и машинное обучение для автоматизации выявления подозрительных связей.

Помимо технологий, пересматриваются и структуры органов. В МВД РФ после Указа Президента Российской Федерации от 30 сентября 2022 г. №688 «О внесении изменений в некоторые акты Президента Российской Федерации» создано «Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий», которому поручено предупреждение, раскрытие преступлений, совершаемых с использованием высоких технологий, и координация в этой сфере [1].

Одним из важных критериев противодействия цифровому отмыванию становится обмен информацией между странами и совместные операции. Точечные успехи достигаются тогда, когда правоохранители разных стран объединяют данные – сведения о транзакциях, IP-логах, обменниках, а для системного эффекта нужны международные соглашения об обмене финансовой информацией в режиме онлайн, синхронизация санкционных списков, признание преступлений с цифровыми валютами, подлежащими экстрадиции и взаимной правовой помощи.

Таким образом, на глобальном уровне есть понимание серьёзности вызовов цифрового отмывания и уже предпринимаются первые важные шаги в правовой, технической, организационной сфере. Тем не менее, стоят и серьёзные вызовы: необходимо не переусердствовать с контролем, сохранив баланс с правами граждан, не отстать от стремительно развивающихся технологий, закрыть пробелы между юрисдикциями. А риски, охарактеризованные выше, требуют стратегического и опережающего подхода.

Заключение. Цифровизация финансовой сферы имеет двойственный характер: с одной стороны, она повышает эффективность и доступность услуг, с другой – создаёт новые ниши для преступной активности. Проведенное исследование подтвердило, что современные технологии – от криптовалют и DeFi до онлайн-игр и краудфандинговых платформ – активно используются злоумышленниками для отмывания денег и финансирования терроризма. Их привлекательность состоит во встроенной трансграничности, относительной анонимности и трудностях правового регулирования. Результаты анализируемых кейсов показали, что преступники выстраивают многоуровневые схемы, совмещая разные инструменты для максимального затруднения отслеживания. Например, криптовалюты и миксеры применяются для скрытия источника средств, децентрализованные платформы – для усложнения цепочек и арбитража между юрисдикциями, NFT и цифровые товары – для маскировки криминальных доходов под легальные транзакции, краудфандинг и соцсети – для рассредоточения финансирования террористических ячеек.

Противодействовать этой “тёмной стороне” цифровизации можно лишь комплексно, сочетая правовые и технологические меры. Необходимо дальнейшее совершенствование законодательства в сфере ПОД/ФТ с учётом появления новых цифровых продуктов. Следует устранять правовые пробелы: вводить понятия криптовалюты и связанных операций в национальные кодексы, устанавливать ответственность за нарушения (как это уже делает Верховный суд РФ, распространяя действие статей об отмывании на криптовалютные схемы [18]). Международные стандарты (рекомендации FATF по виртуальным активам) нужно имплементировать повсеместно и без задержек, чтобы ликвидировать арбитраж возможностей между странами. В 2022-2024 гг. видны положительные сдвиги: FATF обновила руководство по регулируемым криптоактивам, Министерство финансов США выпустило оценку рисков по NFT-сектору, OFAC применило санкции против криптомиксеров. Однако этого недостаточно – требуются новые глобальные соглашения, в том числе о динамическом обмене данными по подозрительным кошелькам и транзакциям, о взаимном признании мер надзора.

С технологической стороны, приоритетом должно стать внедрение передовых инструментов аналитики. Речь идёт об использовании больших данных, алгоритмов машинного обучения, блокчейн-форензики для автоматического выявления аномалий и связей в финансовых потоках. Национальные финразведки (пример – российский “Прозрачный блокчейн”) нужно интегрировать с банковскими системами мониторинга, чтобы подозрительные активности в крипто и фиатном секторах отслеживались во взаимосвязи. Перспективным направлением является создание расширенного цифрового профиля клиентов

с агрегированием информации из разных источников (банковские операции, налоговые данные, имущество) для определения типичного финансового поведения и автоматического флага при резких отклонениях. Реализация таких механизмов требует слаженной работы банков, надзорных органов и ИТ-компаний.

Важнейшая составляющая – опережающий характер противодействия. Регуляторы и правоохранители должны постоянно мониторить появление новых технологических трендов (DeFi 2.0, метавселенные, AI-трейдинг и т.д.), чтобы оценивать потенциальные злоупотребления. Необходимо инвестировать в подготовку кадров: экспертов по кибербезопасности, аналитиков данных, следователей с пониманием блокчейн-технологий. Частному сектору – банкам, финтех-компаниям – следует активно участвовать в обмене информацией о новых типах угроз, повышать квалификацию своих подразделений комплаенс. Только при условии тесного взаимодействия государства и бизнеса можно охватить все “точки входа”, которые могут эксплуатировать преступники. Одновременно требуется информирование общественности: граждане и предприниматели должны понимать, какие риски несёт работа с нелегальными платформами, как не стать невольным пособником (например, сдавая свои документы мошенникам-дропперам).

Итак, тёмная сторона цифровизации – это серьезный и многоаспектный вызов современности. Развитие глобальных правил и стандартов, усиление международной координации, применение инновационных технологий против преступников – всё это формирует основу для успеха. Рекомендации, сформулированные в статье, будет наиболее эффективны, если действовать на опережение, проактивно и сообща. Цифровые технологии будут и дальше эволюционировать, а значит и злоумышленники не остановятся в поиске лазеек. Наша задача – сделать так, чтобы выигрыш от использования новых технологий в преступных целях стал минимальным, а неизбежность выявления – максимальной. Лишь комплексный и скоординированный подход обеспечит устойчивость финансовой системы перед лицом современных цифровых угроз.

Список источников

1. В структуре МВД России создано Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий // Рамблер URL: https://news.rambler.ru/politics/49437030-v-strukture-mvd-rossii-sozdano-upravlenie-po-organizatsii-borby-s-protivopravnym-ispolzovaniem-informatsionno-kommunikatsionnyh-tehnologiy/ (дата обращения: 26.09.2025).

2. Власти США объявили «Криптонеделю» для принятия законов. Что на повестке // РБК URL: https://amp.rbc.ru/crypto/news/6867ac899a7947ce92f67e17 (дата обращения: 27.09.2025).

3. Влияние новых технологий на финансирование терроризма // КиберЛенинка. URL: https://cyberleninka.ru/article/n/vliyanie-novyh-tehnologiy-na-finansirovanie-terrorizma (дата обращения: 26.09.2025).

4. Единая информационная система в сфере противодействия легализации (отмыванию) доходов // TADVISER URL: https://www.tadviser.ru/index.php/Продукт:Единая_информационная_система_в_сфере_противодействия_легализации_%28отмыванию%29_доходов?ysclid=mgttkqotwk794987677 (дата обращения: 25.09.2025).

5. Иванов В.В., Петров С.С., Сидоров А.А. Экономическая безопасность: учебник для вузов. – Москва: Юрайт, 2022. – 500 с.

6. Котельвин М. О. Прозрачный блокчейн: тенденции развития государственного контроля за использованием криптовалюты в преступной деятельности // Право и государство: теория и практика. 2022. №°10 (214). - С.138-13.

7. Курьянов А. М. Цифровизация надзорной деятельности в сфере ПОД/ФТ // Вестник МФЮА. 2023. №4. - С. 37-49.

8. Кучумов А. В., Печерица Е. В. Цифровые инновации, соответствующие требованиям ПОД/ФТ и риск-ориентированный подход // Экономический вектор, 2022. №4. URL: https://cyberleninka.ru/article/n/tsifrovye-innovatsii-sootvetstvuyuschie-trebovaniyam-pod-ft-i-risk-orientirovannyy-podhod

9. Министерство финансов США (OFAC). Press release: U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash (08.08.2022). URL: https://home.treasury.gov/news/press-releases/jy0916 (дата обращения: 01.10.2025)

10. Министерство финансов США. Illicit Finance Risk Assessment of Non-Fungible Tokens (отчёт, май 2024). URL: https://home.treasury.gov/system/files/136/Illicit-Finance-Risk-Assessment-of-Non-Fungible-Tokens.pdf (дата обращения: 01.10.2025)

11. В Томской области выявили организатора канала по финансированию терроризма // Тасс URL: https://tass.ru/proisshestviya/23332751 (дата обращения: 25.09.2025)

12. Новая схема отмывания доходов через игровую валюту // AMLClub. URL: https://amlclub.ru/novaya-shema-otmyvaniya-dohodov-cherez-igrovuju-valjutu/ (дата обращения: 01.10.2025)

13. Палата представителей США приняла пакет из трех законов о криптовалюте // Forbes URL: https://www.forbes.ru/finansy/542126-palata-predstavitelej-ssa-prinala-paket-iz-treh-zakonov-o-kriptovalute (дата обращения: 27.09.2025)

14. США ввели санкции против Blender.io // Тасс URL: https://tass.ru/ekonomika/14565483 (дата обращения: 25.09.25)

15. США исключили Tornado Cash из санкционного списка // Forbes URL: https://www.forbes.ru/finansy/533275-ssa-isklucili-tornado-cash-iz-sankcionnogo-spiska (дата обращения: 25.09.2025)

16. Что такое «Прозрачный блокчейн» и зачем он нужен // Bitget URL: https://www.bitget.com/ru/news/detail/12560604769571 (дата обращения: 25.09.25)

17. Davis J. Illicit Money: Financing Terrorism in the 21st Century. London: Lynne Rienner, 2021. – p. 5.

18. Financial Action Task Force (FATF). Financing of Terrorism through Crowdfunding [Electronic resource]. Paris: FATF, 2023. Available at:
https://www.fatf-gafi.org/en/publications/Financingterrorism/Crowdfunding.html
(date of reference: 12.12.2025).

19. Hetzer Wolfgang Elekronische Geldwasche/ Kriminalistik, BRD, 2002, Ne 2, S. 123-126 // перевод Н.П. Климовой. - М.: ВНИИ МВД России, 2003.

20. Howcroft E. Illicit crypto addresses received at least $24.2 bln in 2023 – report. Reuters, 18.01.2024. URL: https://www.reuters.com/technology/illicit-crypto-addresses-received-least-242-bln-2023-report-2024-01-18/ (дата обращения: 01.10.2025)

21. Howell John. The Prevention of Money Laundering and Terrorist Financing / John Howell ; ill. by David Langdon ; ICC Commercial Crime Services. — Barking : ICC Commercial Crime Services, 2006. — 669 p. : ill. — ISBN 92-842-0002-4.

Сведения об авторах

Малюгина Мария Дмитриевна, студент 3 курса, Финансовый университет при Правительстве Российской Федерации, Москва, Россия.

Сергеева Виолетта Сергеевна, студент 3 курса, Финансовый университет при Правительстве Российской Федерации, Москва, Россия.

Чернышова Елена Николаевна, студент 3 курса, Финансовый университет при Правительстве Российской Федерации, Москва, Россия.

Научный руководитель: **Сударикова Ирина Александровна,** канд. экон. наук, доцент, Финансовый университет при Правительстве Российской Федерации, Москва, Россия.

Information about the authors

Malyugina Maria Dmitrievna, 3rd year student, Financial University under the Government

of the Russian Federation, Moscow, Russia.

Sergeeva Violetta Sergeevna, 3rd year student, Financial University under the Government of the Russian Federation, Moscow, Russia.

Chernyshova Elena Nikolaevna, 3rd year student, Financial University under the Government of the Russian Federation, Moscow, Russia.