Дата поступления рукописи в редакцию: 20.09.2026 г. DOI: 10.24412/2782-3830-2026-11-324-330
Дата принятия рукописи в печать: 12.11.2026 г.

НИКОЛАЕВ Вадим Александрович,
МГУ имени М. В. Ломоносова, Москва, Россия,
e-mail: vadyusha_nikolaev7420@mail.ru

ПРАВОВЫЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ ЛЕГАЛИЗАЦИИ (ОТМЫВАНИЮ) ДОХОДОВ (ПОД/ФТ) ПРИ ОБОРОТЕ ЦИФРОВЫХ ВАЛЮТ

Аннотация. *Исследуется противодействие отмыванию доходов и финансированию терроризма при обороте цифровых валют с учётом российской законодательной реформы 2026 года. Цель работы — определить условия юридически обоснованного использования цифрового анализа и информационного сопровождения переводов. Применены формально-юридический метод, системное толкование и сопоставление с подходами ФАТФ. Разграничены цифровая валюта, цифровые финансовые активы и цифровой рубль, превентивная оценка риска и доказывание преступления. Обосновано, что транзакционная связь не заменяет подтверждения принадлежности актива, его преступного происхождения и направленности умысла. Предложена трёхуровневая проверка: идентификация участника, установление происхождения актива и мотивированный выбор правового последствия. Сформулированы предложения по документированию анализа, ответственности посредников и пересмотру ошибочных ограничений с учётом переходных положений законодательства.*

Ключевые слова: *цифровая валюта, легализация преступных доходов, ПОД/ФТ, цифровой анализ, цифровой депозитарий, идентификация, информационное сопровождение переводов, ФАТФ.*

Для цитирования: *Николаев В. А. Правовые аспекты противодействия легализации (отмыванию) доходов (ПОД/ФТ) при обороте цифровых валют // Российский научный вестник. 2026. № 11. С. 324–330.*

NIKOLAEV Vadim Aleksandrovich,
Lomonosov Moscow State University, Moscow, Russia

LEGAL ASPECTS OF ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING IN DIGITAL CURRENCY TRANSACTIONS

Annotation. *The article examines anti-money laundering and counter-terrorist financing in digital currency transactions following Russia's 2026 legislative reform. It aims to identify conditions for the legally sound use of digital analysis and transfer information. The methods include doctrinal legal analysis, systematic interpretation and comparison with FATF approaches. The study distinguishes digital currency, digital financial assets and the digital ruble, as well as preventive risk assessment and proof of a criminal offence. It argues that a transactional link cannot replace evidence of control over an asset, its criminal origin or the relevant intent. A three-level review is proposed: identification of the participant, examination of the asset's origin and a reasoned choice of legal consequences. Recommendations address documentation of analysis, intermediary responsibility and review of erroneous restrictions, taking account of transitional statutory provisions.*

Key words: *digital currency, money laundering, AML/CFT, digital analysis, digital depository, identification, transfer information, FATF.*

For citation: *Nikolaev V. A. Legal aspects of anti-money laundering and counter-terrorist financing in digital currency transactions. Russian scientific bulletin. 2026;(11):324–330. (In Russ.).*

Оборот цифровых валют поставил перед системой противодействия легализации преступных доходов задачу соединить сведения о движении актива с юридически значимой информацией о его владельце и происхождении. Запись в распределённом реестре способна подтвердить перемещение цифровых единиц, однако сама по себе не устанавливает, кто распорядился ими и на каком основании. Поэтому результативность ПОД/ФТ зависит от согласования финансового мониторинга, отраслевых правил оборота и уголовно-правовой оценки конкретного поведения. Е. А. Липин рассматривает отмывание доходов в цифровой экономике как угрозу экономической безопасности, связанную с изменением способов включения преступного дохода в хозяйственный оборот. Для юридического исследования этот подход требует уточнения: какие сведения достаточны для превентивной проверки и какие обстоятельства необходимо доказать для применения ответственности [1].

Временные границы анализа определены состоянием нормативного регулирования на 18 октября 2026 года. Федеральные законы от 4 августа 2026 года № 282-ФЗ «О цифровых валютах и цифровых правах» и № 283-ФЗ, изменивший связанные законодательные акты, сформировали новую основу регулирования профессионального оборота цифровых валют. При этом принятие нормативной модели и её полное применение не совпадают во времени: законодатель установил переходные сроки и отложенное вступление отдельных положений в силу [2]. Это обстоятельство исключает механическое перенесение выводов публикаций 2021–2025 годов о недостатке регулирования на современное состояние рынка.

Цель исследования — определить условия, при которых данные о цифровой валюте могут служить основанием для обоснованного решения в системе ПОД/ФТ. Объектом выступают отношения, складывающиеся при предупреждении использования цифровых валют в противоправной деятельности; предметом — нормы об идентификации, цифровом анализе, информационном сопровождении переводов и юридических последствиях выявленного риска. Использованы формально-юридический метод, системное толкование и сопоставление национального регулирования с международными стандартами. Научная новизна состоит в обосновании трёхуровневой правовой проверки, которая связывает технический результат анализа с конкретным участником и применимой правовой нормой. Предлагаемая модель имеет нормативно-аналитический характер; её эффективность не представляется как подтверждённая эмпирическим исследованием.

Развитие научных подходов. Д. В. Кащеев связывает риски ПОД/ФТ с трансграничностью криптовалютного рынка, недостатками идентификации и использованием цифровых активов на разных этапах движения преступного дохода [4]. Такое описание полезно для определения направлений контроля, но последовательность размещения, расслоения и интеграции следует рассматривать как аналитическую схему, а не обязательный набор признаков состава преступления. Доход может первоначально возникнуть в цифровой форме, а преобразование в рубли не является необходимым условием возникновения антиотмывочного риска.

Г. В. Назаренко группирует индикаторы отмывания по характеристикам транзакций, способам обеспечения анонимности, сведениям об отправителях и получателях, а также источнику средств [5]. Эта классификация позволяет упорядочить разнородные признаки. Её дальнейшее развитие, по нашему мнению, должно состоять в закреплении связи между обнаруженным индикатором, запрашиваемым подтверждением и возможным правовым последствием. Без такой связи перечень признаков превращается в основание для формального отнесения любой необычной операции к подозрительным.

Б. В. Яцеленко и И. С. Шадрихина обращают внимание на трудности уголовно-правовой оценки операций с цифровой валютой и предлагают совершенствовать механизмы противодействия её использованию при отмывании доходов [6]. Значение этой работы состоит в постановке вопроса о согласованности правового регулирования. Вместе с тем оценка совершённого деяния должна строиться на признаках соответствующего состава, а выводы о необходимости изменения закона — отделяться от описания действующего права. Ни необычность технологии, ни несовершенство контроля сами по себе не подтверждают преступный характер операции.

И. Ю. Золин и С. И. Земцова показывают, что при легализации наркодоходов цифровая валюта используется в сочетании с обменными сервисами и способами усложнения транзакционной истории [7]. Их исследование раскрывает значение установления предикатного источника дохода. Однако выявленная в конкретной криминальной среде типология не может автоматически переноситься на всех участников рынка. Один и тот же технологический инструмент допускает различные способы использования, а его правовая оценка зависит от обстоятельств операции и осведомлённости лица.

Отдельное направление представлено работой Д. Е. Медведевой и А. А. Татаурова, посвящённой цифровому рублю и потенциальным рискам легализации доходов [8]. Сопоставление этой пуб-

ликации с исследованиями криптовалют полезно прежде всего для разграничения правовых режимов. Возможность автоматизации расчётов характерна для разных цифровых инструментов, но круг обязанных субъектов, доступность сведений и способы контроля определяются устройством соответствующей системы. Поэтому единое обозначение «цифровые деньги» недостаточно для выбора применимой нормы.

Предмет регулирования и пределы его унификации. В статье под цифровой валютой понимается объект, определяемый законодательством о цифровых валютах и цифровых правах. Важен имущественный характер такого объекта и отсутствие обязанного перед каждым обладателем лица, кроме субъектов, обеспечивающих соблюдение правил соответствующей информационной системы. Цифровые финансовые активы, напротив, удостоверяют предусмотренные законом права. Цифровой рубль относится к российской национальной валюте и действует в иной правовой и организационной среде. Банк России характеризует его как дополнительную форму рубля [9]. Следовательно, правила частного криптовалютного оборота нельзя без специального основания распространять на платформу цифрового рубля.

Понятие виртуального актива в документах ФАТФ имеет функциональное назначение: оно используется для определения рисков и охвата услуг, связанных с такими активами. Руководство ФАТФ 2021 года связывает применение антиотмывочных мер с характером деятельности поставщика услуг, а не только с используемым им наименованием [10]. Национальная юридическая квалификация при этом сохраняет самостоятельное значение. В частности, токен со стабильной стоимостью нельзя относить к цифровой валюте исключительно по факту его использования в расчётах: необходимо исследовать права владельца, наличие обязанного лица и применимость режима иностранных цифровых инструментов.

Седьмой целевой обзор ФАТФ 2026 года показывает, что развитие законодательства не устраняет практических трудностей выявления поставщиков услуг, надзора и применения правила передачи сведений об участниках перевода. В документе также рассматриваются риски операций через внешние кошельки, офшорных сервисов и децентрализованных финансов [11]. Для российского регулирования из этого следует методологический вывод: создание реестра участников и установление обязанностей необходимо оценивать вместе с возможностью проверить их исполнение. Формальное присутствие посредника в регулируемой системе не обеспечивает достоверности каждой совершённой через него операции.

Обязанности участников профессионального оборота. Федеральный закон № 115-ФЗ связывает предупреждение отмывания доходов с идентификацией, внутренним контролем, выявлением соответствующих операций, хранением и передачей информации уполномоченному органу. Круг обязанных организаций и содержание их действий определяются законом [12]. Поэтому личное владение цифровой валютой, профессиональное предоставление услуг и обслуживание расчёта банком требуют различной правовой оценки. Посредник должен исполнять обязанности, относящиеся к его статусу и функции в операции; клиентский договор не создаёт для него полномочий, которых закон не предусматривает.

Реформа 2026 года вводит цифровые депозитарии и организации, осуществляющие обмен цифровых валют, в систему специального регулирования. Как разъяснил Росфинмониторинг 1 сентября 2026 года, с изменениями связаны идентификация клиентов, обновление сведений, применение предусмотренных законом мер и информационное сопровождение переводов [13]. Основное значение этих правил состоит в создании юридически определённой точки взаимодействия между пользователем, инфраструктурой оборота и уполномоченными органами. Однако сведения депозитария об учёте актива и сведения банка о денежном платеже описывают разные части одной операции; их необходимо сопоставлять по сумме, времени, участникам и основанию расчёта.

Самостоятельное место занимает цифровой анализ по статье 35 Закона № 282-ФЗ. Его предмет охватывает проверку актива и адресов-идентификаторов на связь с деятельностью, в отношении которой установлена уголовная или административная ответственность, а также с иными препятствующими обстоятельствами. Закон предусматривает проведение анализа до сделки или операции, а при отсутствии фактической возможности — в установленный внутренними правилами срок, не превышающий трёх рабочих дней. Для ряда посредников обязанность зависит от использования адресов, администрируемых цифровыми депозитариями; привлечение поставщика услуг не переносит на него ответственность обязанного участника [2]. Таким образом, цифровой анализ представляет собой специальную обязанность с определённой сферой применения, а не универсальную обязанность каждого владельца приобретать коммерческий отчёт о риске.

Информационное сопровождение операций и цифровой анализ выполняют взаимосвязанные, но самостоятельные функции. Статья 7.2-1 Закона № 115-ФЗ регулирует получение, передачу, контроль полноты и хранение сведений об участ-

никах операций с цифровыми валютами и цифровыми правами; последствия отсутствия сведений различаются в зависимости от роли соответствующего лица [12]. История движения актива не заменяет информацию о плательщике и получателе, а правильно заполненное поручение не подтверждает законность происхождения актива. Поэтому соблюдение одной процедуры не должно рассматриваться как доказательство исполнения другой.

Из этого следует необходимость разграничивать и ответственность участников. Депозитарий обеспечивает относящиеся к нему учётные и контрольные действия; брокер исполняет собственные обязанности при передаче поручения; банк оценивает доступную ему денежную часть расчёта. Внутренние документы должны устанавливать, какие сведения получены непосредственно, какие поступили от другого участника и какие нуждаются в дополнительной проверке. Предлагаемое распределение не освобождает от самостоятельных требований закона: оно позволяет установить, на каком участке возник информационный разрыв, и кто должен его устранить.

Превентивный риск и уголовно-правовое доказывание. Результат анализа адреса имеет ограниченное юридическое значение. Отмеченная связь с рискованной инфраструктурой может служить поводом для проверки, но не устанавливает автоматически преступное происхождение всех поступивших активов. Необходимо различать непосредственный перевод от известного контрагента и вывод о связи через последовательность промежуточных адресов. Также должны учитываться особенности формирования аналитических данных: объединение адресов в предполагаемую группу, давность метки, неполнота наблюдаемой истории и возможность ошибочной атрибуции. Это не исключает использования анализа, но требует фиксации его допущений.

Уголовно-правовая оценка по статьям 174 и 174.1 УК РФ предполагает установление предусмотренных соответствующей нормой обстоятельств: приобретения имущества преступным путём, действий с ним, требуемой осведомлённости и цели придания правомерного вида владению, пользованию и распоряжению. Различие между статьями связано, в частности, с тем, кем совершено преступление, в результате которого приобретено имущество [14]. Нарушение условий обслуживания или правил профессионального оборота не равнозначно наличию этого состава. Напротив, формально корректное прохождение идентификации не исключает ответственности, если все необходимые признаки доказаны.

Не следует также отождествлять отмывание доходов и финансирование терроризма. При отмывании ключевое значение имеет преступный источник имущества и предусмотренная законом направленность действий. Для финансирования терроризма средства могут иметь первоначально законный источник; оцениваются цели их предоставления, сбора или использования и осознание соответствующих обстоятельств, установленных уголовным законом. Поэтому проверка только истории происхождения актива недостаточна для всего комплекса ПОД/ФТ. Необходима самостоятельная оценка получателя, назначения операции и иных юридически значимых связей без переноса признаков одного состава на другой.

Использование технических сведений в уголовном процессе требует соблюдения правил получения и оценки доказательств. Положения статей 74 и 88 УПК РФ не допускают подмены исследования относимости, допустимости и достоверности ссылкой на авторитет аналитического сервиса [15]. По нашему мнению, при использовании отчёта следует сохранять исходные сведения о транзакциях, дату выгрузки, идентификаторы операций, версию применённого инструмента и описание способа установления связи адресов. Правовая форма включения этих данных в материалы дела определяется процессуальным законом и обстоятельствами их получения; коммерческий отчёт не становится заключением эксперта только вследствие своего названия.

Трёхуровневая модель правовой проверки. Для согласования рассмотренных требований предлагается модель, в которой каждый уровень отвечает на самостоятельный вопрос. Первый уровень устанавливает участника и его отношение к операции. Проверяются личность или сведения об организации, полномочия представителя, применимые сведения о бенефициарном владельце, принадлежность используемых счетов и характер контроля над адресом. Результат этого уровня — подтверждённая либо требующая уточнения связь конкретного лица с активом. Совпадение имени клиента с именем держателя банковского счёта не заменяет проверки иных существенных обстоятельств.

Второй уровень направлен на происхождение актива и экономическое основание операции. Здесь сопоставляются история переводов, документы о приобретении, сведения о майнинге либо ином заявленном источнике, условия договора и расчётные документы. Объём дополнительного запроса должен зависеть от выявленного риска и возможностей клиента представить подтверждение. Устранение сомнений не следует связывать с требованием доказать отсутствие любой противоправной связи за всю историю существования цифровых единиц. Такое требование практически неисполнимо и не позволяет определить, какое

именно обстоятельство подлежит проверке.

Третий уровень заключается в выборе юридически обоснованного решения. Обязанный участник должен установить норму, определяющую последствие, фактическое основание её применения, необходимый объём фиксации и компетентное лицо, принимающее решение. Продолжение обслуживания, дополнительная проверка, направление сведений уполномоченному органу и предусмотренное законом ограничение — различные результаты. Самостоятельно установленный процент риска не создаёт нового основания замораживания или конфискации имущества. При наличии прямой обязанности закон должен исполняться; при наличии оценочного полномочия необходимы мотивировка и документирование.

Модель можно пояснить на условном примере, который не воспроизводит конкретное уголовное дело. Клиент предъявляет договор продажи ранее приобретённой цифровой валюты, но анализ показывает опосредованную связь адреса с сервисом, отмеченным как рискованный. Первый уровень требует установить отношение клиента к адресу и расчёту. Второй — проверить документируемую историю приобретения и характер выявленной связи. Третий — определить применимое правовое основание дальнейших действий. Если обнаружена ошибка атрибуции, оценка должна быть пересмотрена; если получены обстоятельства, предусмотренные законом для обязательной меры, она применяется независимо от объяснений клиента. Вывод о виновности при этом остаётся за пределами полномочий обслуживающей организации.

Документирование и гарантии прав участников. Практическим инструментом модели предлагается сделать протокол правовой проверки операции. В нём целесообразно фиксировать проверяемый актив и адреса, источники сведений, выявленные индикаторы, документы клиента, проверенные объяснения, применённую норму и принятое решение. Отдельно указываются пределы вывода: подтверждённый факт, вероятностная связь или неустранённое сомнение. Протокол не должен создавать видимость достоверности путём механического заполнения формы. Его назначение — обеспечить возможность установить, почему конкретное ограничение было признано необходимым и какие сведения могут повлиять на пересмотр решения.

Открытость такого решения имеет законные пределы. Часть 6 статьи 35 Закона № 282-ФЗ ограничивает раскрытие правил цифрового анализа; антиотмывочное законодательство также предусматривает ограничения информирования клиента. Поэтому предложение об объяснимости не предполагает передачи клиенту внутренних алгоритмов, закрытых индикаторов или сведений, раскрытие которых запрещено. Следует разграничить защищаемую методику и доступную в установленном порядке информацию о правовом основании решения и способе его пересмотра. Для надзорного и судебного контроля должны сохраняться данные, позволяющие проверить обоснованность действий без публичного раскрытия защищаемых сведений.

При объединении информации об адресах с идентификационными данными возникают обязанности по защите персональных данных. Статьи 5 и 6 Федерального закона № 152-ФЗ требуют учитывать цель, объём и правовое основание обработки [16]. Публичность распределённого реестра сама по себе не означает допустимости любого последующего профилирования идентифицированного лица. Вместе с тем выполнение установленной законом обязанности нельзя ставить в зависимость от произвольного отзыва согласия, если применяется самостоятельное законное основание обработки. При передаче сведений аналитическому поставщику необходимо определить предмет обработки, меры защиты и допустимость доступа к данным.

Переходные положения и направления совершенствования. Применение новых правил требует проверки даты возникновения обязанности. Согласно статье 56 Закона № 282-ФЗ, часть 3 статьи 1, статья 21 и часть 1 статьи 30 вступают в силу 1 июля 2027 года; ряд других положений, включая статью 45, — 1 сентября 2027 года [2]. Поэтому на дату исследования нельзя описывать весь предусмотренный законом режим как уже действующий в полном объёме. В частности, будущие специальные механизмы предотвращения операций без добровольного согласия клиента необходимо отличать от действующих мер ПОД/ФТ. Сроки приведения деятельности отдельных категорий участников в соответствие с новым регулированием также оцениваются по относящимся к ним переходным нормам.

Первое направление совершенствования состоит в установлении требований к проверяемости результата цифрового анализа. Целесообразно определить минимальный состав сохраняемых данных, порядок фиксации версии модели и обновления атрибуции адресов, правила проверки существенных ошибок. Эти требования должны обеспечивать последующий контроль, сохраняя предусмотренную законом конфиденциальность методик. Обязанность доказать надлежащее исполнение контрольной процедуры не тождественна обязанности раскрыть алгоритм всем участникам рынка.

Второе направление — согласование ин-

формационных обязанностей на стыке инфраструктур. Следует предусматривать сопоставимые идентификаторы операции и порядок устранения расхождений между сведениями депозитария, брокера и банка. При этом повторное получение документов может быть оправданно самостоятельной обязанностью участника или противоречием в данных; устранение дублирования не должно превращаться в автоматическое доверие любому сообщению посредника. Для международного обмена необходимы совместимые форматы, законное основание передачи и проверка доступности требуемых сведений у иностранного контрагента.

Третье направление связано с защитой от ошибочного ограничения. В пределах действующих процедур необходимо обеспечить подачу дополнительных сведений, регистрацию обращения, повторную проверку существенной ошибки и фиксацию результата пересмотра. Внутренняя процедура должна учитывать запреты на раскрытие информации и случаи, когда организация не вправе самостоятельно отменить применённую меру. Оценивать качество системы целесообразно по полноте документирования и своевременности законных действий, а также по выявленным и исправленным ошибкам. Количество отказов само по себе не показывает, насколько результативно предотвращается отмывание доходов.

Заключение. Правовые аспекты ПОД/ФТ при обороте цифровых валют определяются сочетанием имущественного режима актива, обязанностей профессиональных участников и правил применения ответственности. Реформа 2026 года создаёт инфраструктуру идентификации, информационного сопровождения переводов и цифрового анализа, однако не устраняет необходимости проверять фактическое основание каждого решения. Транзакционная связь, принадлежность актива и преступное происхождение дохода представляют собой различные обстоятельства. Для финансирования терроризма самостоятельное значение сохраняют назначение средств и предусмотренная законом осведомлённость лица.

Предлагаемая трёхуровневая модель связывает установление участника, проверку происхождения актива и мотивированный выбор правового последствия. Её практическое назначение — обеспечить прослеживаемость решения от исходного сигнала до применённой нормы, сохраняя различие между вероятностной оценкой и доказанным обстоятельством. Развитие регулирования следует ориентировать на проверяемость цифрового анализа, согласованность действий посредников и исправление существенных ошибок. Такой подход позволяет применять меры ПОД/ФТ соразмерно установленным обстоятельствам и в пределах компетенции соответствующего участника.

Список литературы:

[1] Липин Е. А. Влияние легализации доходов, полученных преступным путем на экономическую безопасность страны, в условиях цифровой экономики // Смирновские чтения – 2025: сборник материалов XXIV Международной научно-практической конференции, Санкт-Петербург, 19–21 марта 2025 г. СПб.: Международный банковский институт имени Анатолия Собчака, 2025. С. 266–275.

[2] Федеральный закон от 04.08.2026 № 282-ФЗ «О цифровых валютах и цифровых правах» // Собрание законодательства РФ. 2026. № 32. Ст. 4479.

[3] Федеральный закон от 04.08.2026 № 283-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу законодательных актов (отдельных положений законодательных актов) Российской Федерации» [Электронный ресурс]. URL: https://base.garant.ru/414700473/ (дата обращения: 18.10.2026).

[4] Кащеев Д. В. Противодействие отмыванию денег и финансированию терроризма, обусловленное развитием рынка криптовалют // Вестник Евразийской науки. 2022. Т. 14. № 1. Ст. 32ECVN122. URL: https://esj.today/PDF/32ECVN122.pdf (дата обращения: 18.10.2026).

[5] Назаренко Г. В. Идентификация отмывания доходов, полученных преступным путем с применением цифровых валют // Философия права. 2021. № 4 (99). С. 149–154.

[6] Яцеленко Б. В., Шадрихина И. С. Противодействие использованию цифровой валюты в легализации (отмывании) денежных средств // Лоббирование в законодательстве. 2024. Т. 3. № 3. С. 59–63. DOI: 10.33693/2782-7372-2024-3-3-59-63. EDN: LRJIIQ.

[7] Золин И. Ю., Земцова С. И. Легализация (отмывание) наркодоходов: использование цифровой валюты // Теория и практика противодействия наркоугрозе. 2023. № 4 (20). С. 5–14. DOI: 10.51980/2686-939X_2023_4_5..

[8] Медведева Д. Е., Татауров А. А. Цифровой рубль и легализация денежных средств, полученных преступным путем [Электронный ресурс]: электронная копия публикации. С. 224–230. URL: https://elibrary.ru/item.asp?id=88583499 (дата обращения к электронной копии: 18.10.2026).

[9] Банк России. Что такое цифровой рубль, зачем он и как работает [Электронный ресурс]. URL: https://www.cbr.ru/faq/dr/ (дата обращения: 18.10.2026).

[10] FATF. Updated Guidance for a Risk-Based

Approach to Virtual Assets and Virtual Asset Service Providers. Paris: FATF, 2021. URL: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html (дата обращения: 18.10.2026).

[11] FATF. Seventh Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs. Paris: FATF, 2026. URL: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-updated-virtualassets-vasps-2026.html (дата обращения: 18.10.2026).

[12] Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» // Собрание законодательства РФ. 2001. № 33 (ч. 1). Ст. 3418.

[13] Росфинмониторинг. Федеральная служба по финансовому мониторингу информирует об изменениях в нормативном правовом регулировании, вступающих в силу с 1 сентября 2026 г. [Электронный ресурс]. 01.09.2026. URL: https://fedsfm.ru/releases/10237 (дата обращения: 18.10.2026).

[14] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Собрание законодательства РФ. 1996. № 25. Ст. 2954.

[15] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ // Собрание законодательства РФ. 2001. № 52 (ч. 1). Ст. 4921.

[16] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства РФ. 2006. № 31 (ч. 1). Ст. 3451.

References:

[1] Lipin E.A. The impact of legalization of proceeds from crime on the economic security of the country in the digital economy // Smirnov Readings - 2025: collection of materials from the XXIV International Scientific and Practical Conference, St. Petersburg, March 19-21, 2025 St. Petersburg: Anatoly Sobchak International Banking Institute, 2025. S. 266-275.

[2] Federal Law of 04.08.2026 No. 282-FZ "On Digital Currencies and Digital Rights" // Collection of Legislation of the Russian Federation. 2026. № 32. Art. 4479.

[3] Federal Law of 04.08.2026 No. 283-FZ "On Amending Certain Legislative Acts of the Russian Federation and Invalidating Legislative Acts (Certain Provisions of Legislative Acts) of the Russian Federation" [Electronic Resource]. URL: https://base.garant.ru/414700473/ (access date: 18.10.2026).

[4] Kashcheev D.V. Countering money laundering and terrorist financing due to the development of the cryptocurrency market // Bulletin of Eurasian Science. 2022. T. 14. № 1. Art. 32ECVN122. URL: https://esj.today/PDF/32ECVN122.pdf (Accessed: 18.10.2026).

[5] Nazarenko G.V. Identification of laundering of proceeds from crime using digital currencies // Philosophy of law. 2021. № 4 (99). S. 149-154.

[6] Yatselenko B.V., Shadrikhina I.S. Countering the use of digital currency in the legalization (laundering) of funds // Lobbying in legislation. 2024. VOL. 3. № 3. S. 59-63. DOI: 10.33693/2782-7372-2024-3-3-59-63. EDN: LRJIIQ.

[7] Zolin I. Yu., Zemtsova S. I. Legalization (laundering) of drug profits: the use of digital currency // Theory and practice of countering the drug threat. 2023. № 4 (20). S. 5-14. DOI: 10.51980/2686-939X_2023_4_5..

[8] Medvedeva D.E., Tataurov A.A. Digital ruble and legalization of funds obtained by criminal means [Electronic resource]: electronic copy of the publication. S. 224-230. URL: https://elibrary.ru/item.asp?id=88583499 (electronic copy access date: 18.10.2026).

[9] Bank of Russia. What is a digital ruble, why it and how it works [Electronic resource]. URL: https://www.cbr.ru/faq/dr/ (access date: 18.10.2026).

[10] FATF. Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Paris: FATF, 2021. URL: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html (access date: 18.10.2026).

[11] FATF. Seventh Targeted Update on Implementation of the FATF Standards on Virtual Assets / VASPs. Paris: FATF, 2026. URL: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-updated-virtualassets-vasps-2026.html (access date: 18.10.2026).

[12] Federal Law of 07.08.2001 No. 115-FZ "On Combating the Legalization (Laundering) of Proceeds from Crime and the Financing of Terrorism" // Collection of Legislation of the Russian Federation. 2001. No. 33 (part 1). Art. 3418.

[13] Rosfinmonitoring. The Federal Financial Monitoring Service informs about changes in regulatory legal regulation that come into force on September 1, 2026. [Electronic resource]. 01.09.2026 URL: https://fedsfm.ru/releases/10237 (accessed on: 18.10.2026).

[14] Criminal Code of the Russian Federation of 13.06.1996 No. 63-FZ // Collection of Legislation of the Russian Federation. 1996. № 25. Art. 2954.

[15] Code of Criminal Procedure of the Russian Federation of 18.12.2001 No. 174-FZ // Collection of Legislation of the Russian Federation. 2001. No. 52 (part 1). Art. 4921.

[16] Federal Law of 27.07.2006 No. 152-FZ "On Personal Data" // Collection of Legislation of the Russian Federation. 2006. No. 31 (part 1). Art. 3451.