

Дата поступления рукописи в редакцию: 24.03.2026 г.
Дата принятия рукописи в печать: 14.04.2026 г.

DOI: 10.24412/2782-3830-2026-3-78-82

ИЗУТИНА Светлана Викторовна,

к. ю. н, доцент,
кафедра гражданско-правовых дисциплин
РЭУ имени Г. В. Плеханова,
e-mail: lana.2029@mail.ru

СЕРЕГИН Дмитрий Олегович,

Высшая школа права,
студент 4 курс РЭУ им. Г.В. Плеханова,
e-mail: dima.seregin.04@mail.ru

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИДЕНТИФИКАЦИИ УЧАСТНИКОВ ТРАНСГРАНИЧНЫХ ОПЕРАЦИЙ С ЦИФРОВЫМИ АКТИВАМИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. В статье исследуются правовые проблемы идентификации участников трансграничных операций с цифровыми активами в контексте российского законодательства о противодействии отмыванию денег и финансированию терроризма. Анализируются нормы Федеральных законов № 115-ФЗ и № 259-ФЗ, международные стандарты Группы разработки финансовых мер борьбы с отмыванием денег и отечественные регуляторные инициативы. Предлагаются правовые механизмы решения выявленных проблем.

Ключевые слова: цифровые активы, трансграничные операции, противодействие отмыванию денег, идентификация клиентов, Группа разработки финансовых мер борьбы с отмыванием денег, Федеральная служба по финансовому мониторингу, Федеральный закон № 115-ФЗ, Федеральный закон № 259-ФЗ.

IZUTINA Svetlana Viktorovna,

to. n, Associate Professor, Department of Civil Law Disciplines,
Plekhanov Russian University of Economics

SEREGIN Dmitry Olegovich,

Higher School of Law, 4th year student
of PRUE named after G.V. Plekhanov

LEGAL REGULATION OF IDENTIFICATION OF PARTICIPANTS IN CROSS-BORDER TRANSACTIONS WITH DIGITAL ASSETS IN THE RUSSIAN FEDERATION

Annotation. The article examines legal issues of identification of participants in cross-border transactions with digital assets in the context of Russian legislation on anti-money laundering and countering the financing of terrorism. The analysis covers provisions of Federal Laws No. 115-FZ and No. 259-FZ, international standards of the Financial Action Task Force, and domestic regulatory initiatives. Legal mechanisms for solving identified problems are proposed.

Key words: digital assets, cross-border transactions, anti-money laundering, customer identification, Financial Action Task Force, Federal Financial Monitoring Service, Federal Law No. 115-FZ, Federal Law No. 259-FZ.

Стремительное развитие цифровых технологий и их интеграция в мировую финансовую систему обусловили появление новых видов активов, таких как цифровые финансовые активы и криптовалюты. Трансграничный характер операций с указанными активами и

высокая степень анонимности их владельцев создают не только новые возможности для международной торговли и инвестиций, но и существенные риски, связанные с легализацией доходов, полученных преступным путем, и финансированием терроризма. В этих условиях вопросы

идентификации и верификации участников операций с цифровыми активами приобретают особую актуальность для национальных и международных регуляторов.

Российская Федерация, активно интегрируясь в глобальную цифровую экономику, столкнулась с необходимостью адаптации законодательства к новым вызовам. Принятие Федерального закона от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» и поправок в Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее – Федеральный закон № 115-ФЗ) [2] заложило правовую основу для регулирования оборота цифровых активов. Однако технологические особенности криптовалют, такие как псевдоанонимность и использование некастодиальных кошельков, создают серьёзные препятствия для эффективного правоприменения. Некастодиальные (или самостоятельные) кошельки позволяют пользователям полностью контролировать свои активы без участия посредников, например банков или бирж. При создании такого кошелька генерируется уникальная seed-фраза (обычно 12 или 24 слова), которая является мастер-ключом ко всем приватным ключам и, соответственно всем средствам пользователя. Владение этой фразой равносильно владению активами. Это создаёт фундаментальную проблему для регуляторов: отсутствует централизованный субъект, на которого можно было бы возложить обязанность по идентификации клиента (KYC). В случае если транзакция с такого анонимного кошелька оказывается связана с противоправной деятельностью, установление личности владельца и привлечение его к ответственности становится крайне затруднительным, так как адрес кошелька в блокчейне сам по себе не содержит персональных данных.

Целью настоящей статьи является анализ правовых проблем применения требований ПОД/ФТ и процедуры «Знай своего клиента» (Know Your Customer, далее – ЗСК) при осуществлении трансграничных операций с цифровыми активами в российской юрисдикции, а также формулирование предложений по совершенствованию нормативно-правового регулирования в данной сфере.

Ключевую роль в формировании глобальных стандартов ПОД/ФТ играют рекомендации Группы разработки финансовых мер борьбы с отмыванием денег (Financial Action Task Force, далее – ФАТФ). В июне 2019 года ФАТФ распространила свои требования на поставщиков услуг в сфере виртуальных активов (Virtual Asset Service

Providers, далее – ВАСП), к которым относятся криптовалютные биржи, обменные пункты и операторы кастодиальных кошельков. Центральным элементом этих требований стала имплементация Рекомендации 16, известной как «правило путешествия» (Travel Rule). Суть этого правила заключается в том, что при осуществлении перевода виртуальных активов на сумму, превышающую установленный порог (как правило, 1000 долларов США/евро), ВАСП-отправитель обязан получить, сохранить и передать ВАСП-получателю точную информацию об отправителе и получателе транзакции. Эти сведения включают ФИО, номера счетов (адреса кошельков) и, в зависимости от юрисдикции, адрес или иные идентификационные данные. Таким образом, создаётся информационный след, аналогичный традиционным банковским переводам, что лишает криптовалютные транзакции анонимности и повышает их прозрачность для правоохранительных и надзорных органов [3].

Процесс имплементации обновлённых рекомендаций ФАТФ в российское законодательство проходил поэтапно. После публикации требований Группы в 2019 году, ключевым шагом стало принятие в 2020 году Федерального закона № 259-ФЗ, который ввёл в правовое поле понятия цифровых финансовых активов (ЦФА) и цифровой валюты. Вслед за этим были внесены поправки в Федеральный закон № 115-ФЗ, согласно которым операторы информационных систем, в которых осуществляется выпуск ЦФА, и операторы обмена ЦФА были отнесены к числу организаций, осуществляющих операции с денежными средствами или иным имуществом. В силу статьи 7 указанного закона на них была возложена обязанность проводить идентификацию клиентов, их представителей и выгодоприобретателей до начала обслуживания, а также направлять сведения о подозрительных операциях в уполномоченный орган – Федеральную службу по финансовому мониторингу (далее – Росфинмониторинг).

Вместе с тем практическая реализация требований ЗСК при трансграничных операциях с цифровыми активами сопряжена с рядом правовых и технологических проблем.

Первая проблема связана с псевдоанонимностью блокчейн-транзакций. Несмотря на то, что транзакции в большинстве блокчейнов являются публичными, они привязаны не к реальным именам участников, а к псевдоанонимным адресам. Установление связи между адресом и конкретным физическим или юридическим лицом требует применения специальных аналитических инструментов. При этом действующее нормативно-правовое регулирование не предусматривает обязанности владельцев некастодиальных

кошельков проходить процедуру идентификации. Это создаёт значительные правовые и регуляторные риски, что подтверждается статистикой: по данным Росфинмониторинга, в последние годы наблюдается двукратный рост подозрительных операций с использованием криптовалют, в основном связанных с наркоторговлей и мошенничеством [6]. Согласно отчёту аналитической компании Chainalysis за 2024 год, объём незаконных транзакций в мире в 2023 году достиг \$24,2 млрд [7].

Вторая проблема обусловлена использованием некастодиальных кошельков. В отличие от счетов на централизованных биржах, пользователи децентрализованных сервисов могут создавать и контролировать некастодиальные кошельки без участия посредника. Это значительно усложняет идентификацию владельцев таких кошельков, поскольку отсутствует субъект, на которого возложена обязанность проводить процедуру ЗСК в соответствии со статьей 7 Федерального закона № 115-ФЗ.

Третья проблема связана с применением миксеров и анонимных криптовалют. Существуют специализированные сервисы (миксеры), позволяющие затруднить отслеживание транзакций путем смешивания криптовалюты из различных источников. Кроме того, существуют криптовалюты с повышенной анонимностью (например, Monero, Zcash), которые изначально скрывают информацию об отправителе, получателе и сумме транзакции. Применение подобных инструментов в настоящее время прямо не ограничено российским законодательством, что существенно снижает эффективность мер ПОД/ФТ и указывает на наличие нормативного пробела, требующего правового урегулирования [5].

Четвертая проблема носит юрисдикционный характер. Трансграничные операции предполагают, что участники сделки могут находиться в различных юрисдикциях с различными требованиями к ПОД/ФТ. Это создает сложности с гармонизацией подходов к идентификации и обмену информацией между регуляторами разных государств. Глава IV Федерального закона № 115-ФЗ предусматривает международное сотрудничество в сфере ПОД/ФТ, однако механизмы такого сотрудничества применительно к цифровым активам нуждаются в дальнейшей конкретизации.

В ответ на указанные проблемы российские регуляторы разрабатывают новые инструменты контроля. Ключевой инициативой Росфинмониторинга стала разработка аналитической системы «Прозрачный блокчейн». Согласно официальной информации, данная программа для ЭВМ предназначена для анализа и отслеживания криптовалютных транзакций, деанонимизации их участни-

ков и оценки рисков [4]. Сервис позволяет отслеживать криптовалютную активность клиента, производить оценку риска его операций и определять профиль участника. Начиная с 2023 года, Росфинмониторинг проводил пилотный проект по интеграции «Прозрачного блокчейна» с банковской платформой «Знай своего клиента» (ЗСКК) с участием крупнейших банков. Тестирование было завершено в конце 2025 года, и в 2026 году планируется дальнейшая интеграция сервиса в национальную антиотмывочную систему [6]. Данная интеграция позволит банкам в режиме реального времени выявлять связи между операциями клиентов с фиатными деньгами и криптовалютой, оценивать риски и применять соответствующие меры, предусмотренные статьей 7 Федерального закона № 115-ФЗ. Российская система «Прозрачный блокчейн» является государственным аналогом коммерческих платформ для блокчейн-аналитики, таких как американская Chainalysis или британская Elliptic, которые широко используются финансовыми учреждениями и госорганами по всему миру. Ключевое отличие российской разработки заключается в её статусе государственной информационной системы, интегрированной напрямую в контур национальной системы ПОД/ФТ, что предполагает более тесное взаимодействие между регулятором и поднадзорными организациями.

На данный момент в проекта с участием крупнейших банков тестируется сервис «Знай своего криптоклиента» (далее – ЗСКК), интегрирующий данные системы «Прозрачный блокчейн» с банковской платформой «Знай своего клиента». Данная интеграция позволит банкам выявлять связи между операциями клиентов с фиатными деньгами и криптовалютой, оценивать риски и применять соответствующие меры, предусмотренные статьей 7 Федерального закона № 115-ФЗ, вплоть до отказа в проведении подозрительных транзакций. Так, по итогам проведения данного проекта будет актуально формирование методических подходов и рекомендаций. [4].

Представляется, что для повышения эффективности правового регулирования необходимо принятие следующих мер.

Во-первых, следует дополнить Федеральный закон № 259-ФЗ нормами, устанавливающими обязанность операторов платформ по обмену ЦФА и цифровой валюты проводить углубленную идентификацию клиентов при выводе средств на не верифицированные счета. Это позволит создать правовую основу для контроля за движением цифровых активов за пределы регулируемого сектора.

Во-вторых, необходимо законодательно закрепить запрет на использование миксеров и

анонимных криптовалют при осуществлении операций с участием российских граждан и организаций. Данная мера согласуется с практикой ряда зарубежных юрисдикций и позволит снизить риски использования цифровых активов в противоправных целях.

В-третьих, необходимо развивать международное сотрудничество в сфере обмена информацией о трансграничных операциях с цифровыми активами, уделяя приоритетное внимание взаимодействию с партнёрами из дружественных юрисдикций. Целесообразно развивать положения Главы IV Федерального закона № 115-ФЗ положениями, регулирующими порядок взаимодействия Росфинмониторинга с уполномоченными органами государств — членов ЕАЭС и БРИКС по вопросам идентификации участников криптовалютных транзакций и обмена аналитической информацией в целях противодействия отмыванию доходов и финансированию терроризма.

В-четвертых, необходимо повышение уровня цифровой грамотности всех участников финансового рынка. Росфинмониторингу совместно с Центральным банком Российской Федерации следует разработать методические рекомендации для организаций, осуществляющих операции с ЦФА, по применению риск-ориентированного подхода к идентификации клиентов.

Вместе с тем, при совершенствовании регулирования важно соблюдать баланс между необходимостью контроля и созданием условий для технологических инноваций. Чрезмерно жёсткие меры, такие как полный запрет некастодиальных кошельков или определённых технологий, могут замедлить развитие перспективных направлений, таких как сектор децентрализованных финансов (DeFi) и рынок невзаимозаменяемых токенов (NFT). Поэтому целесообразно сосредоточиться на развитии риск-ориентированного подхода и технологий надзора (SupTech), которые позволяют выявлять высокорисковые операции, не создавая избыточных барьеров для добросовестных участников рынка.

Применение требований ПОД/ФТ и ЗСК к трансграничным операциям с цифровыми активами в российской юрисдикции представляет собой сложную правовую задачу. С одной стороны, создана необходимая законодательная база, соответствующая международным стандартам ФАТФ. С другой стороны, технологические особенности цифровых активов, такие как псевдоанонимность и возможность использования некастодиальных кошельков и миксеров, создают серьезные препятствия для эффективной идентификации и верификации участников сделок.

Инициативы Росфинмониторинга и Центрального банка Российской Федерации, в частности создание платформы «Прозрачный блокчейн» и тестирование сервиса «Знай своего криптоклиента», являются актуальным ответом на существующие риски. Использование риск-ориентированного подхода и современных технологий анализа больших данных позволяет повысить прозрачность криптовалютных операций и выявлять подозрительную активность.

Тем не менее для успешного противодействия незаконным финансовым операциям с использованием цифровых активов необходимо дальнейшее совершенствование нормативной правовой базы. Важнейшими направлениями работы должны стать: законодательное закрепление обязанности углубленной идентификации при выводе средств на некастодиальные кошельки; запрет использования миксеров и анонимных криптовалют; развитие международного сотрудничества по обмену информацией; разработка методических рекомендаций по применению риск-ориентированного подхода. Только комплексный подход позволит найти баланс между стимулированием инноваций и обеспечением экономической безопасности государства.

Список литературы:

- [1] Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства РФ, 03.08.2020, № 31 (часть I), ст. 5018.
- [2] Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» // Собрание законодательства РФ, 13.08.2001, № 33 (часть I), ст. 3418.
- [3] FATF (2021), Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris, France, URL: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html> (дата обращения: 23.02.2026).
- [4] Программа для ЭВМ «Прозрачный блокчейн. Государственный модуль» // Федеральная служба по финансовому мониторингу. URL: <https://www.fedsfm.ru/activity/informational-systems/pb-gos-modul> (дата обращения: 23.02.2026).
- [5] Котельвин Максим Олегович Прозрачный блокчейн: тенденции развития государственного контроля за использованием криптовалюты в преступной деятельности // Право и государство: теория и практика. 2022. №10 (214). URL: <https://cyberleninka.ru/article/n/prozrachnyy-blok>

cheyn-tendentsii-razvitiya-gosudarstvennogo-kontrolya-za-ispolzovaniem-kriptovalyuty-v-prestupnoy-deyatelnosti (дата обращения: 23.02.2026).

[6] Завершено тестирование сервиса криптопроверки в банках «Прозрачный блокчейн» // Интерфакс. 29.12.2025. URL: <https://www.interfax.ru/russia/1065670> (дата обращения: 23.02.2026).

[7] The 2024 Crypto Crime Report // Chainalysis. 18.01.2024. URL: <https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/> (дата обращения: 23.02.2026).

References:

[1] Federal Law of 31.07.2020 No. 259-FZ "On Digital Financial Assets, Digital Currency and on Amendments to Certain Legislative Acts of the Russian Federation" // Collection of Legislation of the Russian Federation, 03.08.2020, No. 31 (Part I), Art. 5018.

[2] Federal Law of 07.08.2001 No. 115-FZ "On Combating Legalization (Laundering) of Proceeds from Crime and Financing of Terrorism" // Collection of Legislation of the Russian Federation, 13.08.2001, No. 33 (Part I), Art. 3418.

[3] FATF (2021), Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset

Service Providers, FATF, Paris, France, URL: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html> (дата обращения: 23.02.2026).

[4] Computer program "Transparent blockchain. State module" // Federal Service for Financial Monitoring. URL: <https://www.fedsfm.ru/activity/informational-systems/pb-gos-modul> (дата обращения: 23.02.2026).

[5] Kotelvin Maxim Olegovich Transparent blockchain: trends in the development of state control over the use of cryptocurrency in criminal activity // Law and state: theory and practice. 2022. №10 (214). URL: <https://cyberleninka.ru/article/n/prozrachnyy-blokcheyn-tendentsii-razvitiya-gosudarstvennogo-kontrolya-za-ispolzovaniem-kriptovalyuty-v-prestupnoy-deyatelnosti> (дата обращения: 23.02.2026).

[6] Testing of the crypto verification service in Transparent Blockchain banks has been completed // Interfax. 29.12.2025 URL: <https://www.interfax.ru/russia/1065670> (accessed on: 23.02.2026).

[7] The 2024 Crypto Crime Report // Chainalysis. 18.01.2024 URL: <https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/> (accessed on: 23.02.2026).



**ЮРИДИЧЕСКОЕ ИЗДАТЕЛЬСТВО
«ЮРКОМПАНИ»**

Издание учебников,
учебных и методических
пособий, монографий,
научных статей.

Профессионально.

В максимально
короткие сроки.

Размещаем
в РИНЦ, E-Library.

ЮРКОМПАНИ

www.law-books.ru