

Вестник Евразийской науки / The Eurasian Scientific Journal <https://esj.today>

2025, Том 17, № s6 / 2025, Vol. 17, Iss. s6 <https://esj.today/issue-s6-2025.html>

URL статьи: <https://esj.today/PDF/35FAVN625.pdf>

5.2.3. Региональная и отраслевая экономика (экономические науки)

Ссылка для цитирования этой статьи:

Прокофьев, Д. И. Риски экономической безопасности операций с криптовалютой / Д. И. Прокофьев // Вестник евразийской науки. — 2025. — Т. 17. — № s6. — URL: <https://esj.today/PDF/35FAVN625.pdf>.

For citation:

Prokofyev D.I. Economic security risks of cryptocurrency transactions. *The Eurasian Scientific Journal*. 2025;17(s6): 35FAVN625. Available at: <https://esj.today/PDF/35FAVN625.pdf>. (In Russ., abstract in Eng.).

УДК 336.7

Прокофьев Денис Игоревич

ПАО «НК «Роснефть», Москва, Россия

Менеджер Службы безопасности

E-mail: d.prokofyev@mail.ru

Риски экономической безопасности операций с криптовалютой

Аннотация. Статья посвящена комплексному исследованию рисков, составляющей использования криптовалютных инструментов в современных социально-экономических условиях. Автором проводится глубокий анализ специфических угроз, генерируемых имманентными характеристиками децентрализованных платежных систем. Особое внимание уделяется выявлению корреляционных зависимостей между структурными особенностями блокчейн-технологий и потенциальными векторами противоправного использования цифровых активов. Исследование фокусируется на детальном рассмотрении многоаспектной природы вызовов экономической безопасности, возникающих при циркуляции криптовалют. Анализируются механизмы реализации деструктивных сценариев, связанных с анонимизацией финансовых потоков, трансграничным характером транзакций и недостаточной зрелостью нормативно-правовых режимов регулирования. Детальному изучению подвергаются способы инкорпорации цифровых валют в схемы легализации доходов, полученных преступным путем, финансирования террористических организаций и обхода международных санкционных ограничений. Значительный акцент сделан на исследовании институциональной реакции регуляторных органов различных юрисдикций на вызовы, продуцируемые криптоэкономикой. Рассматриваются инициативы законодательных и исполнительных властей по формированию комплексной системы контроля, включающей лицензирование участников рынка, введение требований идентификации пользователей и мониторинг подозрительных операций. Анализируются актуальные тенденции в российской правоприменительной практике, включая позиционирование регулятора относительно легитимизации криптовалютных расчетов во внешнеэкономической деятельности.

Автором представлена систематизация ключевых рисков, ассоциированных с майнинговой деятельностью и функционированием децентрализованных финансовых протоколов. Исследуются взаимосвязи между технологическими параметрами консенсусных механизмов и уязвимостями инфраструктуры к манипулятивным воздействиям. Обосновывается необходимость выработки сбалансированного подхода к регулированию, учитывающего как инновационный потенциал технологии распределенных реестров, так и императивы обеспечения финансовой стабильности национальных экономических систем.

Ключевые слова: криптовалюта; цифровые финансовые активы; экономическая безопасность; блокчейн-технология; децентрализованные платежные системы; финансовый мониторинг; легализация преступных доходов; трансграничные транзакции; регуляторная среда

Введение

Криптовалютный рынок демонстрирует устойчивый рост. В России, занимающей одну из лидирующих мировых позиций по объёмам майнинга, криптовалюты используются как средство обхода санкций и осуществления трансграничных платежей. Эти процессы ставят под вопрос стабильность и регулирование банковской системы на фоне отключения от международной платежной инфраструктуры.

При этом, по словам первого заместителя председателя ЦБ РФ Владимира Чистюхина, на сегодняшний день в России фактически операции с криптовалютой находятся в «серой» зоне.¹

Согласно позиции Министра финансов РФ Антона Силуанова, расчеты с использованием крипторынка является большим направлением работы, поскольку с их помощью возможна как оплата, так и вывод валюты из страны. Поэтому, вместе с легализацией этого рынка необходимо усиление контрольных функций со стороны регулятора.²

Помимо этого, тема контроля за обращением криптовалюты видится актуальной в связи с развитием цифровой экономики согласно Указу Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы», что в совокупности обуславливает необходимость всесторонней экономико-правовой оценки использования участниками рынка криптовалют.

С 1 января 2021 г. в России вступил в силу Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте», определяющий термин «цифровая валюта», одной из разновидностью которой является криптовалюта, которая также не имеет материального воплощения и не является денежной единицей, но признается активом и средством платежа.

Базой майнинга выступает технология блокчейн, обеспечивающая проведение транзакций с криптовалютами. Возрастающая популярность криптоактивов стала фактором для разработки нормативно-правовых режимов их обращения; регуляторная реакция во многом связана с обеспокоенностью по поводу потенциального использования криптовалют в преступной деятельности, включая коррупционные схемы, в условиях относительной анонимности транзакций.

В декабре 2025 года Генеральная прокуратура подала в Зюзинский районный суд Москвы иск об обращении в доход государства активов бывших сотрудников Бюро специальных технических мероприятий МВД России. По версии следствия, фигуранты получили крупнейшую в истории ведомства взятку — 5 млрд руб., переданных в криптовалюте администратором биржи World Exchange Services Pte. Ltd. (Wex, прежняя BTC-e) за предоставление «крыши».³

¹ ЦБ: внешнеторговые расчеты в криптовалютах не получили широкого применения. URL: https://www.alta.ru/external_news/122822/ (дата обращения: 12.12.2025).

² Силуанов рассказал о легализации криптовалюты во внешней торговле. URL: <https://ria.ru/20251021/rossiya-2049664813.html> (дата обращения: 12.12.2025).

³ Генпрокуратура потребовала изъять имущество рекордсмена по взяткам в МВД. URL: <https://www.forbes.ru/finansy/51104-genprokuratura-potrebovala-iz-at-imustvo-rekordsmena-po-vzatkam-v-mvd> (дата обращения: 16.12.2025).

Статистические данные по уголовным делам в Свердловской области указывают на значительную долю преступлений в сфере незаконного оборота наркотиков, связанных с использованием криптовалют. По данным исследований, криптовалюты также задействованы в отдельных эпизодах коррупционных преступлений и телефонного мошенничества, а также хищений с банковских счетов.⁴

Согласно письму Банка России от 03.03.2022 № 05-35-2/1340 «О комментариях АРБ по консультативному докладу Банка России о криптовалютах», отсутствие адекватных инструментов мониторинга оборота криптовалюты может привести к увеличению доли сделок в теневом секторе экономики и способствовать усилению криминогенных факторов в Российской Федерации.

Таким образом, криптовалюта представляет собой не только объект совершения коррупционных правонарушений, но и средство их реализации. Исходя из этого, требуется всесторонний анализ антикоррупционных аспектов контроля за оборотом криптовалюты в России и за рубежом.

1. Методы и материалы

Эмпирическую основу составляет совокупность официальных документов регуляторных органов Российской Федерации, включая нормативные акты Центрального Банка, Министерства финансов и профильных ведомств, курирующих вопросы противодействия легализации преступных доходов.

В качестве первичных источников использовались материалы публичных выступлений представителей надзорных институтов, официальные пресс-релизы и аналитические обзоры, раскрывающие позицию государственных структур относительно регулирования криптоэкономической сферы. Привлекались данные специализированных информационных ресурсов, мониторящих динамику рынка цифровых активов и фиксирующих инциденты, связанные с компрометацией финансовой безопасности.

Методологический инструментарий включал систематический анализ периодической литературы, посвященной проблематике функционирования децентрализованных финансовых систем таких авторов как: Д.Ю. Данилова [1], А.С. Гардалоева [2], Ю.И. Юриной [3], В.В. Качалова [4], А.Х. Цакаева [5], А.Г. Коринного [6], И.В. Деревцовой [7], А.В. Лебедевой [8], Е.Л. Гринько [9], Н.В. Сафина [10], Н.В. Капустиной [11], Е.Л. Гринько [12], А.М. Рабаданова [13], Д.А. Кочергина [14], С.В. Лемайкиной [15].

2. Результат и обсуждение

Несмотря на увеличение степени государственного регулирования возрастающих объемов криптовалютных сделок, единообразная позиция в отношении статуса криптовалюты в мире отсутствует, так как каждое государство самостоятельно определяет нормативно-правовую базу в отношении криптовалютного рынка, а подходы зарубежных регуляторных органов по данному вопросу отличаются.

Отсутствие географических ограничений упрощает перемещение средств между юрисдикциями с разным уровнем регулирования. Это создаёт «регуляторные лакуны», которые коррупционеры могут использовать для легализации доходов.

⁴ Прокурор разъясняет. URL: <https://epp.genproc.gov.ru/ru/gprf/activity/legal-education/explain/> (дата обращения: 16.12.2025).

Европейское управление по ценным бумагам и рынкам (ESMA) отмечает, что регуляторные органы Европейского Союза должны вводить обязательные требования по раскрытию информации о рисках при проведении Initial Coin Offerings (ICO), с тем чтобы повысить прозрачность эмиссий токенов, защитить инвесторов и снизить системные риски, связанные с распространением неконтролируемых цифровых предложений.⁵

В последние годы в европейском правовом пространстве наблюдается активная разработка и внедрение комплексных нормативных мер, направленных на регулирование обращения криптоактивов и минимизацию сопутствующих рисков. Регулирование охватывает несколько взаимосвязанных направлений:

1. Правовой статус и надзор за криптоактивами. Введён ряд нормативов, определяющих правовой статус различных типов токенов, обязанности поставщиков услуг по обращению с криптоактивами (exchanges, custodians, провайдеры кошельков), а также критерии разграничения инвестиционных и нефинансовых токенов. Это позволяет привязать отдельные операции с криптоактивами к профильным режимам регулирования и надзора.

2. Защита прав потребителей и инвесторов. Регламенты требуют раскрытия существенной информации о рисках эмиссии токенов (включая ICO), гарантий надёжности платформ, механизмов хранения и возможностей возврата средств. Установлены стандарты информационной прозрачности и обязанностей по предотвращению конфликтов интересов.

3. Обеспечение финансовой стабильности и управления системными рисками. Нормативы ориентированы на выявление и снижение рисков концентрации, операционных рисков и распространения шоков между традиционными финансовыми институтами и рынком криптоактивов. Для этого применяются требования к лимитам, процедурам стресс-тестирования и раскрытию рисков системного характера.

4. Противодействие финансовым преступлениям. Особое внимание уделяется AML/KYC-обязательствам для криптопосредников, порядку ведения учёта и обмена информацией о подозрительных транзакциях. Регламентация деятельности операторов электронных платформ и обменников направлена на снижение возможностей использования сервисов для отмывания, финансирования терроризма и сокрытия коррупционных платежей.

5. Технологическая и институциональная адаптация. Евроинституты стимулируют внедрение методов блокчейн-аналитики, применение механизмов контроля транзакций в реальном времени, а также развитие сотрудничества между регуляторами, правоохранительными органами и частным сектором в целях оперативного обмена данными и совместных расследований.

Вместе с тем ряд уязвимостей сохраняется и требует внимания:

1. Уязвимость пользователей и P2P-транзакций. Хотя регулируемые платформы всё чаще подпадают под надзор, участники P2P-операций и пользователи децентрализованных сервисов остаются вне централизованных процедур KYC/AML, что делает их потенциальными «слабым звеном» для вовлечения в коррупционные или иные преступные схемы.

2. Юрисдикционный разрыв и арбитраж. Операторы и сервисы, зарегистрированные в другом государстве или полностью децентрализованные, могут использовать различия в национальном регулировании для обхода ограничений и обеспечения анонимности клиентов.

3. Технические обходные методы. Миксеры, тамблеры, «цепочная» миграция средств (chain-hopping) и использование конфиденциальных блокчейнов существенно усложняют трассируемость операций и требуют всё более совершенных инструментов аналитики.

⁵ Криптовалюты и блокчейн как атрибуты новой экономики. URL: <https://ecc.eaeunion.org/upload/medialibrary/704/Doklad.pdf> (дата обращения: 19.12.2025).

4. Баланс регулирования и инноваций. Чрезмерно жёсткие меры могут подавлять технологическое развитие и оттеснить активность в менее контролируемые юрисдикции, тогда как излишняя либерализация увеличивает риски злоупотреблений.

Рыночная практика подтверждает актуальность проблемы отсутствия единообразной регуляторной политики в отношении статуса криптовалюты в мире. В частности, отмечаются напряженные отношения криптовалютного гиганта Tether с регуляторными органами.⁶ В США компания готова соблюдать новый Genius Act, регулирующий криптовалюты, запуская стейблкоин USAT и направляя USDT на развивающиеся рынки.⁷ В то же время в Европейском союзе она заявила, что не будет соблюдать закон MiCA (Markets in Crypto-Assets), что привело к запрету на размещение USDT на европейских биржах.⁸

По данным аналитической компании Chainalysis, в 2024 году 63 % незаконных транзакций в блокчейне проводились через стейблкоины, прежде всего криптовалюта USDT.⁹

Это «криптовалюта, излюбленная организованной преступностью Восточной и Юго-Восточной Азии», — говорится в отчёте Управления ООН по наркотикам и преступности (УНП ООН) от января 2024 года.¹⁰ USDT активно применяется в схемах нелегальных онлайн-гемблингов и в мошенничествах типа pig butchering, описанных журналистом Зиком Фоксом в книге Number Go Up (W&N, 2023). В ответ Tether в сентябре 2024 года создала специальную рабочую группу совместно с исследовательской фирмой TRM Labs и блокчейном Tron для быстрого реагирования на незаконные транзакции.¹¹

Однако эффективность данной инициативы вызывает сомнение, так как по состоянию на август 2024 года в Tether работало всего около 100 человек, что, даже с учетом планов увеличения штата работников до 200 человек к 2025 году, резко контрастирует с масштабом и прибылью компании и делает невозможным удовлетворить все запросы на блокировку.¹²

Отсутствие законодательного регулирования обращения инновационных продуктов и цифровых прав за рубежом, а также отсутствие ясного правового статуса смарт-контрактов затрудняют эффективное противодействие криминальным практикам, связанным с операциями в сфере криптоактивов. В международной плоскости это проявляется в нескольких ключевых аспектах:

⁶ Согласно отчёту Tether за второй квартал 2025 года, её активы в казначейских облигациях США оцениваются в \$127 млрд: \$105,5 млрд в прямых активах и ещё \$21,3 млрд в косвенных, что делает Tether одним из крупнейших держателей американского госдолга. Режим доступа — URL: <https://ru.investing.com/news/cryptocurrency-news/article-2856748> (дата обращения: 05.01.2026).

⁷ CEO Tether подтвердил сроки выхода компании на рынок США. Режим доступа — URL: <https://forklog.com/new/s/ceo-tether-podtverdil-sroki-vyhoda-kompanii-na-rynok-ssha> (дата обращения: 05.01.2026).

⁸ MiCA: Новый этап регулирования крипторынка в ЕС. Режим доступа — URL: <https://www.ixbt.com/live/crypto/mica-novyy-etap-regulirovaniya-kriptorynka-v-es.html> (дата обращения: 05.01.2026).

⁹ Более \$40 млрд в криптовалютах было получено незаконно в 2024 году. Режим доступа — URL: <https://www.rbc.ru/crypto/news/6788d1249a7947c7393ae148?from=copy> (дата обращения: 05.01.2026).

¹⁰ Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat. Режим доступа — URL: https://www.unodc.org/roseap/uploads/documents/Publications/2024/Casino_Underground_Banking_Report_2024.pdf (дата обращения: 05.01.2026).

¹¹ Tether, TRON and TRM Labs Establish First-Ever Private Sector Financial Crime Unit to Combat Crypto Crime. Режим доступа — URL: <https://tether.io/news/tether-tron-and-trm-labs-establish-first-ever-private-sector-financial-crime-unit-to-combat-crypto-crime/> (дата обращения: 06.01.2026).

¹² К 2025 году штат сотрудников Tether увеличится вдвое: взгляд изнутри на стратегическое расширение эмитента USDT. Режим доступа — URL: <https://www.binance.com/ru/square/post/12039877249434> (дата обращения: 06.01.2026).

- правовая неоднородность и пробелы: различные юрисдикции по-разному квалифицируют цифровые права, токены и смарт-контракты, что создаёт возможности для юридического арбитража и уклонения от ответственности;
- проблемы идентификации и доказательной базы: смарт-контракты, будучи самовыполняемыми программными объектами, часто функционируют без чёткой привязки к юридическим лицам или лицам-контрагентам, что усложняет установление ответственности и предъявление правовых притязаний;
- сложности изъятия и реализации активов: при отсутствии унифицированных правил обращения с цифровыми правами в разных странах замороженные или конфискованные криптоактивы трудно легитимно конвертировать и передать в пользу пострадавших или государства;
- усиление технических рисков: смарт-контракты могут содержать уязвимости или предусматривать автоматизированные схемы распределения средств (например, мульти-сиг или DAO-структуры), что усложняет оперативное вмешательство и восстановление незаконно выведенных средств.

В совокупности эти факторы повышают стойкость криминальных схем, использующих цифровые права и смарт-контракты, и снижают эффективность национальных мер контроля и правоприменения. Следовательно, обеспечение противодействия злоупотреблениям требует международной координации правового регулирования, в том числе:

1. Гармонизации квалификации цифровых прав и смарт-контрактов на межгосударственном уровне, чтобы сократить возможности для юрисдикционного арбитража.
2. Разработки стандартов для юридического приписывания ответственности сторонам смарт-контрактов (включая провайдеров инфраструктуры и разработчиков), а также процедурных механизмов для приостановления исполнения контрактов в случае подозрения на преступную активность.
3. Внедрения соглашений о международной правовой помощи и оперативном обмене данными для обеспечения доступа к сведениям о транзакциях и контрагентах в разных юрисдикциях.
4. Создания правовых процедур и технических механизмов для учёта, описи, замораживания и реализации цифровых прав и смарт-контрактных активов в интересах государств и потерпевших.
5. Развития технических средств аудита смарт-контрактов и интеграции результатов аудита в надзорные и правоохранительные практики.

Только при сочетании международно-правовой гармонизации, чёткой регламентации смарт-контрактов и усиления технической и организационной базы контроля станет возможным значимо ограничить использование инновационных цифровых инструментов в криминальных схемах при сохранении пространства для законных технологических инноваций.

Криптовалюты позволяют проводить операции без прямого указания личности, что затрудняет идентификацию участников коррупционных сделок. Хотя блокчейн фиксирует транзакции, злоумышленники используют сервисы-миксеры и анонимные кошельки для сокрытия следов. Контроль за обращением криптовалюты становится критически важным в ситуациях, когда коррупционные схемы реализуются с использованием так называемых тамблеров (криптомиксеров). Эти сервисы смешивают входящие транзакции от большого количества пользователей, дробят и перераспределяют средства через многочисленные адреса,

а затем возвращают «очищенные» суммы отправителям за вычетом комиссии. В результате нарушается сквозная прослеживаемость потоков средств: традиционные методы анализа блокчейна, основанные на сопоставлении входов и выходов, теряют эффективность, а связи между источником и получателем средств размываются.

Последствия применения криптомиксеров в коррупционных схемах многочисленны:

- существенное усложнение задач финансового мониторинга и аналитики: автоматизированные системы выявления подозрительных операций (программные фильтры, алгоритмы AML) дают больше ложных срабатываний и чаще нуждаются в ручной проверке;
- затруднение доказательной базы в уголовных и административных делах: следователям сложнее установить причинно-следственные связи между лицами и транзакциями, что снижает вероятность успешного преследования;
- рост транзакционных и процедурных затрат для правоохранительных и контрольных органов из-за необходимости применения специализированных технических средств и международной кооперации;
- увеличение привлекательности криптовалюты как инструмента для сокрытия хищений, взяток и иных злоупотреблений, что подрывает общественное доверие и финансовую стабильность.

Эффективное противодействие использованию тамблеров в коррупционных целях требует сочетания правовых, технологических и международно-правовых мер: введения обязательных требований по раскрытию информации и регистрации операторов сервисов смешивания, усиления требований KYC/AML к криптовалютным платформам и обменникам, развития методик блокчейн-аналитики и обмена разведанными между юрисдикциями, а также рассмотрения правового статуса и уголовно-правовой квалификации деятельности операторов миксеров. Только комплексный подход позволит снизить риски злоупотреблений при одновременном сохранении пространства для легитимных инноваций в сфере цифровых активов.

Следует иметь в виду, что в практическом смысле легитимным владельцем криптовалюты признаётся лицо, обладающее фактическим доступом к соответствующим приватным ключам или иным средствам управления активами, даже если этот доступ был получен преступным путём. Иными словами, право распоряжения средствами в блокчейне определяется не только юридической принадлежностью, но и фактическим контролем над ключами; это обстоятельство осложняет установление и защиту законных прав на цифровые активы и требует учёта при расследовании и нормативном регулировании. Имеющиеся законодательные пробелы регулирования оборота криптовалют являются причиной повышения коррупционных рисков практически во всех юрисдикциях.

Несмотря на признание криптовалюты имуществом, остаются нерешённые вопросы по определению стоимости криптовалюты на момент совершения преступления, порядка наложения ареста и конфискации цифровых активов, а также взаимодействия с международными платформами для получения данных о транзакциях.

В связи с этим усматривается целесообразность обеспечения возможности наложения ареста на цифровые активы, которое хотя и не было получено в результате коррупционного преступления, но были отчуждены третьим лицам для целей их сокрытия и уклонения от возмещения ущерба. При этом для решения проблемы вывода активов за рубеж необходимо проработать отдельный порядок выделения уголовных дел для целей розыска и возврата преступно добытого имущества.

Вопросам обеспечения трансграничного сотрудничества по противодействию коррупции и отмыванию преступных доходов, в том числе связанному с использованием криптовалют и иных цифровых активов в коррупционных схемах, в российской практике отводится ведущая роль Генеральной прокуратуре Российской Федерации. Её функции включают координацию межведомственного взаимодействия, международную правовую помощь, инициирование уголовного преследования и обмен информацией с иностранными правоохранительными и надзорными органами, что делает прокуратуру ключевым звеном в реализации комплексных мер по выявлению, пресечению и расследованию трансграничных финансовых преступлений с применением цифровых технологий.

Скрытый характер передачи криптовалюты должностным лицам в виде взяток и перспективы создания в Российской Федерации государственной цифровой платформы для аккумулирования изъятых активов обуславливают необходимость широкого применения прокуратурой современных аналитических и информационно-поисковых ресурсов. В частности, предполагается активное использование интегрированных систем аналитики (например, «Посейдон») и портала «Национальная система пространственных данных» (НСПД), в который входят сведения об объектах недвижимости, пространственные данные, полученные методом космической и аэрофотосъёмки, и лазерного сканирования, сведения о зарегистрированных правах на недвижимость и данные о государственной кадастровой оценке. Синтез и кросс-анализ этих массивов информации позволяют формировать комплексные индикаторы риска — в том числе выявлять несоответствие между фактическими расходами государственных служащих и их декларируемыми доходами — что повышает оперативную и доказательственную эффективность выявления случаев незаконного обогащения и использования цифровых активов в коррупционных схемах. Кроме того, сочетание геопространственных данных с блокчейн-аналитикой и результатами межведомственного обмена информацией создаёт предпосылки для заблаговременного обнаружения аномалий, ускорения процессуальных действий по изъятию и учёту активов, а также для разработки унифицированных процедур хранения и последующей реализации конфискованных цифровых средств.

Важным компонентом такой аналитической работы должно стать применение методов машинного обучения и алгоритмов выявления аномалий для автоматизированного отбора приоритетных проверок и сокращения числа ложных срабатываний. Не менее существенна интеграция результатов блокчейн-аналитики (трассировка транзакций, идентификация сопряжённых адресов, обнаружение использования миксеров) с геопространственными и реестровыми данными для выявления корреляций между движением цифровых активов и приобретением материальных благ. Для повышения эффективности контроля требуется установление правового механизма доступа к сведениям у иностранных криптовалютных платформ и операторов, включая возможности исполнения межгосударственных запросов о предоставлении данных и замораживании активов на время процессуальных действий.

Роль прокуратуры в этой системе должна сочетаться с усилением межведомственного взаимодействия (финразведка, налоговые органы, МВД, органы по противодействию коррупции) и созданием специализированных экспертных подразделений, обладающих техническими компетенциями для работы с цифровыми доказательствами. Параллельно целесообразно разработать стандартизированные процедуры аудита и оценки цифровых активов, а также регламенты по их хранению, учёту и реализации, что обеспечит прозрачность последующих процедур и минимизирует риск утраты или неправомерного расходования изъятых средств. Наконец, значимым фактором повышения эффективности является правовое закрепление ответственности за сокрытие сведений о владении криптоактивами и за препятствование доступу к ним, включая механизмы процессуального пресечения попыток незаконной конвертации и вывода активов.

В соответствии с Федеральным законом от 26.10.2002 № 127-ФЗ «О несостоятельности (банкротстве)» криптовалюта может рассматриваться как имущество должника и включаться в конкурсную массу с последующей реализацией в ходе процедур банкротства. На практике, однако обезличенность записей в блокчейне и ограниченные возможности идентификации владельцев усложняют исполнение судебных и процессуальных мер: должник может отказать в предоставлении доступа к цифровому кошельку либо заявить о неверных учетных данных, а направленное судебное поручение бирже или требование личной авторизации в присутствии нотариуса не обеспечивает абсолютной гарантии получения контроля над средствами. В результате это создает условия для незаконного вывода криптоактивов из конкурсной массы — в том числе умышленного — и снижает эффективность процедур по взысканию и реализации имущества должника.

Практическую значимость представляют результаты проверок и исковых заявлений прокуратуры Республики Татарстан о взыскании в доход государства цифровых финансовых активов в связи с непредставлением сотрудником органов внутренних дел в декларации сведений, подтверждающих законность приобретения имущества.

Нормативно-правовой базой таких действий служит статья 17 Федерального закона от 03.12.2012 № 230-ФЗ «О контроле за соответствием расходов лиц, замещающих государственные должности, и иных лиц их доходам», согласно которой прокуратура вправе обращаться в суд с требованиями об обращении в доход государства недвижимого имущества, земельных участков, а также цифровых финансовых активов и цифровой валюты, если лицом, замещающим (занимающим) государственную должность, не представлены документы, подтверждающие приобретение имущества на законные доходы.

В одном из рассмотренных прокуратурой Республики Татарстан дел по результатам запросов в ФСБ России, Федеральную службу по финансовому мониторингу (Росфинмониторинг) и Центр цифровых исследований «Цифровой контроль» был установлен факт приобретения бывшим сотрудником органов внутренних дел цифровой валюты, автомобиля и погашения кредита без надлежащего подтверждения их законного источника финансирования. На основании собранных материалов прокуратура предъявила иск о взыскании сумм, эквивалентных стоимости указанных активов, в доход государства. Данный кейс иллюстрирует практический механизм взаимодействия прокуратуры с профильными государственными органами при расследовании возможного незаконного обогащения с использованием цифровых активов: формулирование запросов, анализ блокчейн-транзакций, сопоставление сведений о доходах и расходах, оценка стоимости имущества и подготовка исковой документации.

Однако реализация подобных мер наталкивается на существенные процедурные и институциональные препятствия. Во-первых, криптовалютные биржи и сервисы хранения активов часто находятся за пределами юрисдикции Российской Федерации, что затрудняет получение сведений о владельцах и движении средств, а также исполнение судебных актов. Во-вторых, технические особенности блокчейн-технологий — обезличенность записей, использование миксеров, P2P-переводов и само-схем с множеством адресов — осложняют сбор достоверных доказательств, необходимых для обоснования исковых требований. В-третьих, в российском правовом поле отсутствует отлаженный механизм правового обращения замороженных или конфискованных криптоактивов в доход Российской Федерации: недостаточно регламентированы процедуры описи, хранения, оценивания и реализации таких активов, а также порядок их юридического закрепления за государством после вступления решения суда в законную силу.

Эти трудности порождают ряд практических рисков: увеличение продолжительности и стоимости процедур по взысканию, снижение вероятности успешного исполнения судебных

решений, а также возможность вывода или конвертации активов до момента наложения процессуальных ограничений. Кроме того, отсутствие ясного правового регулирования создает лазейки для уклонения от ответственности и для сокрытия доходов с использованием международных сервисов и криптоинструментов.

Во избежание описанных проблем необходим комплекс мер. Во-первых, требуется совершенствование правовой базы: разработка процедур замораживания, учета и реализации криптоактивов в рамках исполнительных и уголовно-процессуальных механизмов; установление обязанностей по сотрудничеству для российских и иностранных криптобирж и провайдеров услуг хранения; закрепление правового статуса цифровых финансовых активов при процедуре банкротства и в рамках контроля расходов государственных служащих. Во-вторых, необходимо усиление межведомственного и международного взаимодействия: налаживание оперативного обмена информацией с зарубежными регуляторами и платформами, использование каналов международной правовой помощи и совместных расследований. В-третьих, требуются технологические и кадровые меры: внедрение специализированных инструментов блокчейн-аналитики, создание реестров и процедур оценки цифровых активов, а также подготовка специалистов в прокуратуре и правоохранительных органах для работы с цифровыми доказательствами.

Заключение

Таким образом, приведённые практические примеры прокуратуры Республики Татарстан подчёркивают не только наличие фактов незаконного приобретения и обращения цифровых активов без надлежащих подтверждений, но и указывают на необходимость системных изменений в нормативно-процессуальном обеспечении, технической базе и международном сотрудничестве для эффективного обращения в доход государства криптоактивов, связанных с сомнительными доходами государственных служащих. По результатам проведенного в рамках данной работы анализа установлено, что коррупционные риски операций с криптовалютой связаны с её анонимностью, трансграничностью и правовыми пробелами. Для эффективного противодействия необходимо комплексное решение:

1. Принцип «регулировать, а не запрещать» остаётся обоснованным и прагматичным: он позволяет интегрировать криптоактивы в правовую систему, минимизировать риски и одновременно сохранять условия для инноваций. Однако реализация этого принципа требует чёткого набора обязательств для посредников и механизмов контроля.
2. Необходимо усилить регламентацию P2P-операций и децентрализованных сервисов: в том числе внедрять риск-ориентированные требования к провайдерам инфраструктуры (например, провайдеры кошельков, агрегаторы), а также разрабатывать технические средства мониторинга без разрушения принципов приватности легитимных пользователей.
3. Следует обеспечить международную координацию и гармонизацию правил, включая соглашения о сотрудничестве с иностранными биржами и обменниками, механизмы международной правовой помощи и оперативного обмена информацией, что уменьшит возможности юрисдикционного арбитража.
4. Развивать и внедрять технологические инструменты: инвестиции в блокчейн-аналитику, интеграцию AML-систем с аналитикой цепочек, применение инструментов для обнаружения смешивания транзакций и chain-hopping; создание специализированных подразделений в регуляторных и правоохранительных органах.

5. Необходимо разработать процедурный механизм обращения и реализации замороженных или конфискованных криптоактивов, включая стандарты описи, хранения, оценки и реализации, а также пути конвертации активов в национальную валюту с учётом международно-правовых ограничений.
6. Следует внедрить системные меры по повышению финансовой грамотности и осведомлённости пользователей, а также механизмы защиты пострадавших инвесторов и контроль прозрачности маркетинга и представления рисков при ICO и других размещениях.
7. Баланс между контролем и инновациями может быть достигнут через применение риск-ориентированного подхода: более строгий надзор и требования к участникам с высокой рисковой профилем и адаптивные, облегчающие меры для проверенных и прозрачных участников рынка.

Принятие комплексного набора перечисленных мер позволит существенно снизить уязвимости, связанные с использованием криптоактивов в коррупционных и иных преступных схемах, повысить устойчивость кредитно-финансовой системы и создать более предсказуемую и безопасную среду для развития легитимных цифровых инноваций.

ЛИТЕРАТУРА

1. Данилов, Д.Ю. Правовой режим цифровых валют и обеспечение законности в сфере их оборота / Д.Ю. Данилов, Н.Д. Бут // Вестник Университета прокуратуры Российской Федерации. — 2022. — № 1(87). — С. 28–36. — EDN BFKFOC.
2. Гардалоев, А.С. Современные тенденции уголовно-правового обеспечения безопасности цифрового финансового рынка / А.С. Гардалоев — DOI 10.18572/2072-4411-2023-4-16-20. // Уголовное судопроизводство. — 2023. — № 4. — С. 16–20 — EDN DMFYRB.
3. Юрина, Ю.И. Предмет мошенничества с использованием криптовалюты / Ю.И. Юрина // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. — 2023. — № 23-1. — С. 260–261. — EDN ESHPIJ.
4. Качалов, В.В. Получение взятки криптовалютой: вопросы квалификации / В.В. Качалов — DOI 10.31085/2310-8681-2020-2-208-19-25. // Союз криминалистов и кримиологов. — 2020. — № 2. — С. 19–25 — EDN SACTIZ.
5. Цакаев, А.Х. О влиянии криптовалют на экономическую безопасность России / А.Х. Цакаев, М.Р. Хаджиев — DOI 10.18334/ecsec.3.1.110121. // Экономическая безопасность. — 2020. — Т. 3, № 1. — С. 53–62 — EDN FFILNY.
6. Коринной, А.Г. Об отдельных элементах механизма регулирования оборота криптовалюты / А.Г. Коринной — DOI 10.24412/2414-3995-2022-1-271-276. // Вестник экономической безопасности. — 2022. — № 1. — С. 271–276 — EDN GFRHZW.
7. Майнинг как угроза обеспечения экономической безопасности Иркутской области / И.В. Деревцова, А.Н. Грязнов, К.В. Семенцов, Е.Е. Чалов — DOI 10.17150/2411-6262.2022.13(2).29. // Baikal Research Journal. — 2022. — Т. 13, № 2 — EDN FTGJDG.
8. Лебедева, А.В. Современные риски криптоизации экономики / А.В. Лебедева — DOI 10.36807/2411-7269-2022-2-29-118-125. // Экономический вектор. — 2022. — № 2(29). — С. 118–125 — EDN VIFNPJ.

9. Гринько, Е.Л. К вопросу определения рисков криптовалютных активов и операций с ними в платежных системах / Е.Л. Гринько, М.А. Гарагуц // Актуальные вопросы учета и управления в условиях информационной экономики. — 2023. — № 5. — С. 497–501. — EDN HSOTYI.
10. Сафин, Н.В. Потенциальные риски современного криптовалютного рынка и возможности управления ими / Н.В. Сафин, Т.В. Стовбыра // Финансовый менеджмент. — 2024. — № 8. — С. 323–335. — EDN RJTGXX.
11. Капустина, Н.В. Применение технологий искусственного интеллекта и блокчейн-аналитики в системах ПОД/ФТ для мониторинга криптовалютных транзакций / Н.В. Капустина // Вестник евразийской науки. — 2025. — Т. 17, № 4. — EDN HAADRV.
12. Гринько, Е.Л. К вопросу определения рисков криптовалютных активов и операций с ними в платежных системах / Е.Л. Гринько, М.А. Гарагуц // Актуальные вопросы учета и управления в условиях информационной экономики. — 2023. — № 5. — С. 497–501. — EDN HSOTYI.
13. Рабаданов, А.М. Анализ влияния центрального банка и правительственного регулирования на развитие блокчейн-технологии / А.М. Рабаданов // Вестник евразийской науки. — 2023. — Т. 15, № S4. — EDN OPYIZM.
14. Кочергин, Д.А. Криптоактивы: экономическая природа, классификация и регулирование оборота / Д.А. Кочергин — DOI 10.17323/1996-7845-2022-03-04. // Вестник международных организаций: образование, наука, новая экономика. — 2022. — Т. 17, № 3. — С. 75–130 — EDN ISTXME.
15. Лемайкина, С.В. Актуальные вопросы правового регулирования криптовалюты / С.В. Лемайкина // Философия права. — 2025. — № 1(112). — С. 142–146. — EDN PQEOEY.

Prokofyev Denis Igorevich

PJSC NK Rosneft, Moscow, Russia

E-mail: d.prokofyev@mail.ru

Economic security risks of cryptocurrency transactions

Abstract. This article presents a comprehensive study of the risky nature of using cryptocurrency instruments in the current socioeconomic environment. The author conducts an in-depth analysis of the specific threats generated by the inherent characteristics of decentralized payment systems. Particular attention is paid to identifying correlations between the structural features of blockchain technologies and potential vectors for the illegal use of digital assets. The study focuses on a detailed examination of the multifaceted nature of economic security challenges arising from the circulation of cryptocurrencies. The mechanisms for implementing destructive scenarios related to the anonymization of financial flows, the cross-border nature of transactions, and the insufficient maturity of regulatory frameworks are analyzed. This article examines in detail the methods of incorporating digital currencies into money laundering schemes, financing terrorist organizations, and circumventing international sanctions. Significant emphasis is placed on examining the institutional response of regulatory bodies in various jurisdictions to the challenges posed by the cryptoeconomy. Initiatives by legislative and executive authorities to develop a comprehensive control system, including licensing of market participants, introducing user identification requirements, and monitoring suspicious transactions, are examined. Current trends in Russian law enforcement practice are analyzed, including the regulator's positioning regarding the legitimization of cryptocurrency payments in foreign trade. The author presents a systematization of key risk categories associated with mining activities and the functioning of decentralized financial protocols. The relationship between the technological parameters of consensus mechanisms and the vulnerabilities of infrastructure to manipulative influences is examined. The need for a balanced approach to regulation that takes into account both the innovative potential of distributed ledger technology and the imperatives of ensuring the financial stability of national economic systems is substantiated.

Keywords: cryptocurrency; digital financial assets; economic security; blockchain technology; decentralized payment systems; financial monitoring; money laundering; cross-border transactions; regulatory environment