Вестник Восточно-Сибирского института МВД России. 2025. № 4 (115). С. 167–180.
Vestnik of the East Siberian Institute of the Ministry of Internal Affairs of Russia. 2025, vol. 115, no. 4, pp. 167-180.

5.1.4. Уголовно-правовые науки (юридические науки)

Научная статья
УДК 343.7

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА ПРЕСТУПЛЕНИЯ, СОВЕРШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТ

Перетолчин Артём Павлович
Восточно-Сибирский институт МВД России, Иркутск, Российская Федерация, peretart@yandex.ru

Введение. В статье исследуются уголовно-правовые аспекты преступлений, совершаемых с использованием криптовалют, в контексте неопределенности их правового статуса в российском законодательстве. Анализируются проблемы квалификации смешанных составов (хищение, вымогательство, легализация доходов), процессуальные сложности изъятия и конфискации цифровых активов, а также криминогенные характеристики криптовалют, включая их использование в наркоторговле, терроризме и коррупционных схемах. На основе изучения судебной практики, международного опыта (Казахстан, Китай) и технологических особенностей блокчейн-платформ автор выявляет системные противоречия в правоприменении.

Материалы и методы. Материалами исследования послужили научные статьи ученых и специалистов, нормы законодательства Российской Федерации, Китайской Народной Республики, Республики Казахстан, постановления Пленума Верховного Суда Российской Федерации, судебные акты 2018–2024 гг., международные стандарты Группы разработки финансовых мер борьбы с отмыванием денег (англ. Financial Action Task Force, FATF), ведомственные и корпоративные аналитические отчеты и исследования. Методологически исследование опирается на диалектический подход, формально-юридический и системно-структурный анализ, сравнительно-правовой и историко-правовой методы, а также на статистические приемы обработки данных.

Результаты исследования. Проанализированы криминогенные свойства криптовалют (трансграничность, псевдоанонимность, DeFi-механизмы) и выявлены ключевые проблемы правоприменения: неопределенность статуса криптовалютных активов как «иного имущества», коллизии при квалификации смешанных составов (кража / мошенничество / доступ к компьютерной информации), пробелы в механизмах изъятия и конфискации, трудности оценки стоимости активов. Сравнительный обзор зарубежного опыта позволил определить эффективные подходы гибкой модели (Казахстан) и запретительного режима (Китай).

Выводы и заключения. Установлена необходимость четкого нормативного закрепления криптовалюты как объекта имущественных прав, детализации составов преступлений, для совершения которых используются криптовалютные активы, разработки процессуальных инструментов депонирования ключей и блокировки средств на уровне смарт-контрактов, а также интеграции блокчейн-аналитики в следственную практику. Комплексное обновление уголовного и уголовно-процессуального регулирования рассматривается как условие повышения эффективности противодействия кибер- и криптопреступности.

Ключевые слова: уголовная ответственность, криптовалюта, квалификация преступлений, хищение, вымогательство, легализация доходов, блокчейн-анализ, конфискация цифровых активов, DeFi

Для цитирования: Перетолчин, А. П. Уголовная ответственность за преступления, совершаемые с использованием криптовалют // Вестник Восточно-Сибирского института МВД России. 2025. № 4 (115). С. 167–180.

5.1.4. Criminal law sciences (legal sciences)

Original article

CRIMINAL LIABILITY FOR OFFENCES COMMITTED THROUGH THE USE OF CRYPTOCURRENCIES

Artyom P. Peretolchin
East-Siberian Institute of the Ministry of Internal Affairs of the Russian Federation, Irkutsk, Russian Federation, peretart@yandex.ru

Introduction. The article explores the criminal-law dimensions of offences perpetrated with the use of cryptocurrencies against the backdrop of their uncertain legal status in Russian legislation. It analyses issues in classifying hybrid offences (theft, extortion, money-laundering), the procedural difficulties of seizing and confiscating digital assets, and the criminogenic characteristics of cryptocurrencies, including their use in drug trafficking, terrorism and corruption schemes. Drawing on judicial practice, international experience (Kazakhstan, China) and the technological specifics of blockchain platforms, the author identifies systemic contradictions in law enforcement.

Materials and Methods. The research are based on scholarly works, the legislation of the Russian Federation, the People's Republic of China and the Republic of Kazakhstan, plenary resolutions of the Supreme Court of the Russian Federation, court decisions from 2018 to 2024, FATF international standards, as well as departmental and corporate analytical reports. Methodologically, it employs the dialectical approach, formal-legal and systems-structural analysis, comparative-legal and historical-legal methods, and statistical data-processing techniques.

The Results of the Study. The criminogenic properties of cryptocurrencies – cross-border nature, pseudo-anonymity and DeFi mechanisms – were analysed, revealing key enforcement challenges: ambiguity in recognising crypto-assets as “other property”, conflicts in qualifying hybrid offences (theft / fraud / unlawful access to computer information), gaps in seizure and confiscation mechanisms, and valuation difficulties. A comparative review of foreign practice highlighted effective aspects of a flexible model (Kazakhstan) versus a prohibitionist regime (China).

Findings and Conclusions. The analysis underscores the need for clear statutory recognition of cryptocurrency as an object of proprietary rights, detailed regulation of offences involving crypto-assets, procedural tools for key escrow and smart-contract-level freezing of funds, and the integration of blockchain analytics into investigative practice. A comprehensive overhaul of criminal and criminal-procedural regulation is deemed essential for strengthening the fight against cyber- and crypto-enabled crime.

Keywords: criminal liability, cryptocurrency, offence qualification, theft, extortion, money-laundering, blockchain analytics, confiscation of digital assets, DeFi

For citation: Peretolchin, A. P. Ugolovnaya otvetstvennost' za prestupleniya, sovershaemye s ispol'zovaniem kriptovalyut [Criminal Liability for Offences Committed Using Cryptocurrencies]. Vestnik Vostochno-Sibirskogo instituta MVD Rossii – Vestnik of the East-Siberian Institute of the Ministry of Internal Affairs of Russia. 2025, vol. 115, no. 4, pp. 167-180.

Введение цифровых активов в финансовый оборот ознаменовало новый этап развития экономических отношений, сопровождающийся возникновением принципиально иных форм противоправной деятельности. Криптовалюты, обладая уникальными свойствами децентрализации, псевдоанонимности и трансграничности, создали беспрецедентные возможности для совершения и сокрытия преступлений, поставив перед правовыми системами вызовы, требующие комплексного научного осмысления и адекватного законодательного реагирования. В Российской Федерации отсутствие единого подхода к определению правовой природы цифровых валют порождает существенные проблемы в квалификации преступных деяний, процессуальном доказывании и обеспечении имущественных требований, что актуализирует исследование уголовно-правовых аспектов их использования в преступных целях.

Фундаментальной проблемой является неопределенность правового статуса криптовалют в отечественном законодательстве. Несмотря на их активное использование в гражданском обороте, законодатель воздерживается от четкого закрепления правовой природы, что создает коллизии в правоприменительной практике. Как отмечает М. М. Долгиева, криптовалюта в силу специфических свойств, ценности и возможности являться предметом гражданского оборота должна быть

отнесена к видам иного имущества в рамках ст. 128 Гражданского кодекса Российской Федерации[1] (далее – ГК РФ) [1, с. 215].

Противоположную позицию занимает Э. Л. Сидоренко, утверждающая, что из-за отсутствия легальной дефиниции криптовалюты в российском законодательстве ее нельзя признать объектом гражданских прав, а следовательно, любые формы присвоения априори не могут быть признаны хищением [2, с. 130]. Однако необходимо отметить, что данные позиции были высказаны учеными до принятия и вступления в силу Федерального закона от 31 июля 2020 года № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», который дал легальное определение понятию «цифровая валюта». Вместе с тем отраженная в законе дефиниция, на наш взгляд, не отражает в полной мере сущности и значения такого явления, как криптовалюта.

Эта теоретическая и понятийная дискуссия находит непосредственное отражение и в судебной практике. Так, Девятый арбитражный апелляционный суд фактически признал право лица владеть, пользоваться и распоряжаться содержимым криптокошелька как своим собственным имуществом, включив биткоины в конкурсную массу[2]. В 2022 году Санкт-Петербургский городской суд в деле о грабеже признал криптовалюту предметом хищения, квалифицировав ее как «иное имущество» в контексте ст. 128 ГК РФ[3].

Сложности правовой квалификации преступлений с использованием криптовалют выходят далеко за рамки простого определения статуса актива [3, с. 227]. Остро стоит проблема разграничения составов преступлений. Например, хищение криптовалюты путем взлома аккаунта на бирже или перехвата сид-фразы кошелька традиционно квалифицируется по ст. 158 Уголовного кодекса Российской Федерации[4] (далее – УК РФ) как тайное хищение чужого имущества. Однако в случае мошенничества, связанного с фиктивными инвестиционными платформами или «скамом» (преднамеренным обманом для завладения средствами инвесторов), правоприменители часто сталкиваются с искусственной подменой квалификации.

Нередко такие деяния ошибочно относят к мошенничеству в сфере компьютерной информации (ст. 159.6 УК РФ), что не отражает сути преступления, направленного именно на завладение имуществом (криптовалютой), а не на

---

[1] Гражданский кодекс Российской Федерации : ГК : принят Гос. Думой 21 октября 1994 года : послед. ред. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_5142/ (дата обращения: 16.10.2024).

[2] Постановление Девятого арбитражного апелляционного суда № 09АП-16416/2018 от 15 мая 2018 года по делу № А40-124668/2017 // Электронное правосудие : сайт. URL: https://kad.arbitr.ru/Card/3e155cd1-6bce-478a-bb76-1146d2e61a4a (дата обращения: 16.10.2025).

[3] Апелляционное определение Судебной коллегии по уголовным делам Санкт-Петербургского городского суда от 16 мая 2022 года по делу № 22-2616/2022 // Гарант : сайт. URL https://base.garant.ru/328707158/ (дата обращения: 16.10.2025).

[4] Уголовный кодекс Российской Федерации : УК : принят Гос. Думой 24 мая 1996 года : одобрен Советом Федерации 5 июня 1996 года : послед. ред. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 16.10.2025).

неправомерное воздействие на компьютерную информацию. Это порождает дисбаланс в санкциях и не способствует адекватной защите потерпевших.

Исследователи подчеркивают, что квалификация должна исходить из объекта посягательства, которым в подавляющем большинстве случаев выступает именно собственность, а безопасность компьютерных данных является лишь способом совершения преступления [4, с. 83].

Проблема усугубляется при квалификации вымогательства криптовалюты (ст. 163 УК РФ) под угрозой распространения компрометирующих данных или блокировки информационных систем (ransomware-атаки) [5, с. 706]. Требуется четкое толкование Верховного Суда Российской Федерации, разграничивающее составы в зависимости от способа воздействия на потерпевшего и конечной цели преступника – завладения цифровым имуществом.

Особую сложность представляет квалификация смешанных составов:

– при хищении криптовалюты через взлом кошелька вредоносным программным обеспечением деяние требует одновременного применения ст. 159.6 УК РФ (мошенничество в сфере компьютерной информации) и ст. 272 УК РФ (неправомерный доступ);

– вымогательство криптоактивов (ransomware-атаки) не охватывается ст. 163 УК РФ, так как угроза уничтожения данных не входит в диспозицию нормы.

Подходы к квалификации криптопреступлений
в Российской Федерации

Тип деяния	**Доминирующая квалификация**	**Проблемы**
Хищение кошелька	ст. 159.6 УК РФ	Разграничение с кражей (ст. 158 УК РФ)
Вымогательство	ст. 163 УК РФ ст. 272 УК РФ	Отсутствие признака «угроза повреждения данных»
Легализация доходов	ст. 174.1 УК РФ	Определение стоимости при конвертации
Нелегальный обмен	ст. 172 УК РФ	Отнесение обменных операций к банковской деятельности

Однако подобные решения носят казуистический характер и не устраняют системных противоречий. Отсутствие полноценного, соответствующего современным реалиям законодательно закрепленного статуса криптовалюты как объекта преступного посягательства приводит к невозможности единообразной квалификации деяний, связанных с их незаконным завладением, отмыванием или использованием в коррупционных схемах. Правоприменители вынуждены прибегать к расширительному толкованию понятия «имущество».

Технологические особенности блокчейн-платформ предопределяют их привлекательность для противоправного использования. Децентрализованный

характер реестра транзакций, отсутствие единого контролирующего органа и псевдоанонимность участников создают значительные сложности для правоохранительных органов. Как справедливо отмечается в исследованиях, «анонимность, предоставляемая такими криптовалютами, как Monero и ZCash, а также сервисами криптосмешивания, облегчает совершение и сокрытие преступлений» [6, с. 89].

Криптовалюты активно используются в торговле оружием и наркотиками, финансировании терроризма, а также в коррупционных схемах, в рамках которых традиционная классическая взятка уходит в прошлое, уступая место оффшорным транзакциям и операциям с криптовалютами [7, с. 108]. Международные исследования подтверждают, что децентрализация, псевдоанонимность и трансграничный характер криптовалют обеспечивают беспрепятственное движение финансовых потоков и усложняют отслеживание транзакций. Особую опасность представляет эволюция предпочтений преступников: если ранее доминировал Bitcoin, то в последние годы наблюдается активное использование приватных криптовалют (privacy coins) и стейблкоинов, обладающих повышенными конфидентными характеристиками.

По данным аналитической компании Chainalysis (2024), общий объем криптовалют, полученных преступным путем, в 2023 году составил около $24.2 млрд, при этом на долю мошенничества пришлось $8.9 млрд, а на вымогательство – более $1 млрд[1]. Эти цифры, хотя и несколько ниже пиковых значений 2021–2022 гг., свидетельствуют о стабильно высоком уровне криминального использования цифровых активов.

Преобладающей тенденцией последних лет стал рост децентрализованной преступности (DeFi-скамы). Преступники активно эксплуатируют непрозрачность децентрализованных финансовых протоколов (DeFi) для создания фиктивных проектов, организации pump-and-dump схем (искусственное «накачивание» цены токена с последующей распродажей организаторами) и прямого хищения средств через уязвимости в смарт-контрактах.

Как отмечают исследователи, DeFi создал идеальную среду для высокотехнологичного мошенничества, где анонимность разработчиков, отсутствие регуляторного надзора и техническая сложность для рядового пользователя сливаются в единый криминогенный фактор [8, с. 332].

Отдельную и нарастающую угрозу представляют криптовалютные схемы в сфере легализации коррупционных доходов. Использование миксеров (сервисов смешивания транзакций), p2p-платформ, обменников с либеральной KYC-политикой и NFT для отмывания взяток и средств, полученных в результате злоупотреблений должностными полномочиями, требует разработки специализированных методик выявления и доказывания, интегрированных в систему противодействия коррупции.

Отсутствие урегулированного механизма изъятия и конфискации цифровых активов существенно затрудняет расследование преступлений. Законодательные

[1] Crypto Crime Report 2024. // Chainalysis : сайт. URL: https://www.chainalysis.com/reports/crypto-crime-report-2024 (дата обращения: 17.10.2025).

инициативы апреля 2025 года в части изъятия криптовалюты[1] являются очень важным шагом в вопросе урегулирования отдельных аспектов в сфере противодействия криптовалютной преступности, но они не решают всех проблем, особенно в контексте децентрализованных технологий (DeFi) и смарт-контрактов. Конфискация средств, заблокированных в смарт-контрактах (например, в рамках кредитных пулов DeFi, стейкинга или ликвидности), технически крайне затруднительна без сотрудничества обвиняемого или наличия бэкдора в коде контракта, что противоречит самой философии DeFi. Возникает правовая коллизия: как конфисковать то, доступ к чему контролируется алгоритмом, а не лицом?

Аналогичная проблема возникает с активами на некастодиальных кошельках, приватные ключи от которых известны только обвиняемому. Правовая доктрина большинства стран, включая Россию, запрещает принуждение к даче показаний против себя самого (nemo tenetur se ipsum accusare). Это делает невозможным принудительное изъятие ключей, оставляя единственным решением либо добровольную их выдачу (что маловероятно), либо физическое изъятие носителя (аппаратного кошелька) без гарантии доступа к средствам.

Даже при успешном изъятии или переводе криптовалюты на государственный адрес встает проблема ее легальной реализации. Отсутствие у Федеральной службы судебных приставов (далее – ФССП) законодательно закрепленного механизма и инфраструктуры для безопасной и прозрачной продажи конфискованных криптоактивов на открытом рынке создает риски их обесценивания, утраты или даже новых злоупотреблений. Требуется создание специализированного государственного института или уполномоченных криптодепозитариев, обладающих лицензией и технологическими возможностями для хранения, оценки и реализации цифровых активов в пользу бюджета, с соблюдением всех требований финансовой безопасности и прозрачности.

Традиционные меры процессуального принуждения оказываются малоэффективными в отношении виртуальных активов, хранящихся в децентрализованных сетях. В апреле 2025 года власти предварительно одобрили механизм признания криптовалюты имуществом и способы ее изъятия при уголовных делах, что стало значительным шагом вперед. Законопроект предусматривает два основных сценария изъятия: конфискацию материальных устройств, на которых хранится цифровая валюта или код доступа к ней, и перевод криптовалюты на специальный адрес-идентификатор, позволяющий обеспечить ее сохранность. Однако практическая реализация этих мер сталкивается с серьезными техническими и правовыми препятствиями.

При изъятии аппаратных кошельков («холодных» кошельков) возникают сложности с получением ключей доступа, поскольку обвиняемого нельзя принудить к их раскрытию [9, с. 113]. Перевод средств на контролируемый адрес возможен

[1] О внесении изменений в статью 104-1 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации : законопроект № 902782-8 // Система обеспечения законодательной деятельности : сайт. URL: https://sozd.duma.gov.ru/bill/902782-8 (дата обращения: 17.10.2025).

преимущественно при использовании централизованных бирж, сотрудничающих с правоохранительными органами, в то время как децентрализованные платформы и зарубежные сервисы остаются вне зоны доступа. Дополнительную сложность представляет оценка стоимости изымаемых активов, отличающихся исключительной волатильностью, и последующая конвертация конфискованной криптовалюты в фиатные деньги, поскольку ФССП не располагает эффективным механизмом для реализации цифровых активов.

Анализ зарубежной практики регулирования криптовалют выявляет различные подходы к регулированию цифровых активов. В Республике Казахстан в 2020 году был принят закон, согласно которому криптовалюты признали имуществом, что обеспечило защиту прав инвесторов и способствовало притоку капитала в страну [10, с. 183]. В Китае, напротив, установлен запрет на популярные криптовалюты под предлогом борьбы с отмыванием денег и защиты финансовой системы, хотя исследователи отмечают, что действительной причиной является необходимость защиты национальной цифровой валюты – цифрового юаня [11, с. 103].

Значительный интерес представляет практика применения Рекомендации 15 Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ), предусматривающей распространение антиотмывочных мер на виртуальные активы. В Постановлении Пленума Верховного Суда Российской Федерации от 7 июля 2015 года № 32 учтены положения Конвенции Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности, разрешившие вопрос о криптовалюте как предмете легализации денежных средств[1]. Однако этого недостаточно для комплексного решения проблемы трансграничного характера преступлений с использованием криптовалют, что требует развития международного сотрудничества и гармонизации законодательств.

Для преодоления выявленных проблем необходим системный подход, сочетающий законодательные инициативы с развитием следственной и судебной практики. Первоочередной мерой должно стать внесение изменений в ст. 128 ГК РФ, дополняющих категорию «иное имущество» понятием «цифровая валюта». Это создаст правовую основу для единообразной квалификации преступлений против собственности, коррупционных деяний и операций по легализации преступных доходов. Параллельно требуется внесение корректировок в Уголовный и Уголовно-процессуальный кодексы Российской Федерации, детализирующих:

– способы изъятия и конфискации криптовалют с учетом технических особенностей их хранения;

– методики оценки стоимости цифровых активов на момент совершения преступления;

[1] О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем : постановление Пленума Верховного Суда Российской Федерации от 7 июля 2015 года № 32 : ред. от 26 февраля 2019 года // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_182365/ (дата обращения: 15.10.2025).

– процедуры взаимодействия с криптобиржами и провайдерами кошельков;

– механизмы международного сотрудничества при расследовании трансграничных преступлений.

Особое внимание следует уделить разработке и внедрению специализированных инструментов блокчейн-анализа, позволяющих правоохранительным органам отслеживать подозрительные транзакции в публичных реестрах. Преодоление процессуальных барьеров немыслимо без активного внедрения передовых технологий криминалистического блокчейн-анализа и искусственного интеллекта (далее – ИИ). Современные платформы, такие как Chainalysis Reactor, Elliptic, TRM Labs, позволяют не просто отслеживать транзакции, но и выявлять сложные паттерны поведения, кластеризацию адресов, связь с известными криминальными сервисами (миксерами, обменниками с высоким риском) и даже предсказывать вероятные направления движения средств. ИИ-алгоритмы, обученные на огромных массивах данных публичных блокчейнов, способны автоматически идентифицировать подозрительные активности, ассоциированные с вымогательством (транзакции на известные адреса ransomware-групп), фишингом или работой ботнетов.

Однако эффективность этих инструментов резко падает при работе с приватными криптовалютами (Monero, Zcash) и транзакциями, прошедшими через миксеры высокой интенсивности. Это требует не только дальнейшего развития аналитических технологий, но и законодательного закрепления обязанности вендоров приватных криптовалют и DeFi-протоколов внедрять элементы контролируемой прослеживаемости (без ущерба для базовой конфиденциальности легитимных пользователей) в соответствии с международными стандартами.

Также критически важным является развитие международной кооперации в режиме реального времени, создание единых баз данных «криптовалютных отпечатков» преступных схем и упрощение процедур взаимной правовой помощи по делам, связанным с цифровыми активами. Как отмечают эксперты, несмотря на мифы об анонимности криптовалюты, любой пользователь может отследить операции и проверить данные любого криптокошелька в открытых источниках [12, с. 105].

Современные аналитические платформы, использующие big data и машинное обучение, способны выявлять паттерны преступной деятельности, ассоциированные с отмыванием средств, финансированием терроризма и торговлей запрещенными товарами. Важным направлением является обучение сотрудников правоохранительных органов современным методам расследования преступлений в сфере цифровых активов и развитие межведомственного взаимодействия с Росфинмониторингом и финансовыми разведками других стран.

Для преодоления выявленных сложностей представляется целесообразным реализация следующего комплекса мер:

1. Введение в Уголовно-процессуальный кодекс Российской Федерации специальной процедуры «судебного депонирования ключей»: при наличии достаточных оснований полагать, что обвиняемый владеет криптовалютой, полученной преступным путем или используемой в преступных целях, в случае отказа предоставить ключи доступа, суд может обязать его передать ключи или seed-фразу на

хранение в специальный государственный криптодепозитарий под контролем суда или следствия. Уклонение от исполнения такого решения может повлечь самостоятельную уголовную ответственность (по аналогии с неуплатой алиментов или злостным неисполнением решения суда), не нарушая при этом принцип nemo tenetur.

2. Разработка и законодательное закрепление методики оценки криптовалют для целей следствия и суда: необходимо установить единый порядок определения рыночной стоимости актива на момент совершения преступления (например, средняя цена на крупнейших лицензированных биржах в конкретный временной промежуток) и на момент конфискации/реализации.

3. Обязательное назначение криминалистической блокчейн-экспертизы по делам о преступлениях с криптовалютами: Экспертиза должна устанавливать путь движения похищенных средств, их возможную принадлежность к известным криминальным кластерам, факт использования миксеров, связь между адресами и идентифицированными пользователями (через процедуры KYC бирж).

4. Создание в структуре Следственного комитета Российской Федерации и Министерства внутренних дел Российской Федерации специализированных подразделений по расследованию киберпреступлений с фокусом на криптоаналитике, укомплектованных специалистами в области блокчейна, криптографии и финансовых расследований, с постоянным повышением их квалификации и оснащением современными аналитическими инструментами и аппаратными средствами.

5. Развитие института «заморозки» и «блокировки» активов на уровне смарт-контрактов в сотрудничестве с добросовестными разработчиками DeFi-протоколов. Хотя это противоречит принципам децентрализации, в исключительных случаях по решению суда возможно взаимодействие с создателями протоколов (если они идентифицируемы и юрисдикционно доступны) для реализации механизмов временной блокировки подозрительных активов до окончания судебного разбирательства.

Интеграция криптовалют в преступную деятельность представляет собой серьезный вызов для уголовно-правовой системы страны, требующий адекватного и оперативного реагирования. Отсутствие полноценной нормативной урегулированности статуса цифровых валют, противоречивость судебной практики, технологические сложности при изъятии и конфискации виртуальных активов создают благоприятную почву для безнаказанности преступников. Решение этих проблем видится в синтезе законодательных инициатив, технологических инноваций и международного сотрудничества. Признание криптовалют имуществом в уголовно-правовом контексте станет отправной точкой для формирования последовательной правоприменительной практики [13, с. 48], а разработка специализированных методик расследования и внедрение инструментов блокчейн-анализа позволят правоохранительным органам эффективно противостоять новым формам преступности.

Игнорирование этих вызовов чревато не только ростом криптовалютной преступности, но и оттоком капитала и технологических компетенций в юрисдикции с более прогрессивным регулированием, что подтверждается сравнительным анализом

опыта Казахстана и Китая [14, с. 47]. Уголовно-правовая система должна адаптироваться к реалиям цифровой экономики, обеспечивая защиту имущественных прав граждан и экономической безопасности государства в новых технологических условиях.

Таким образом, уголовно-правовое противодействие преступности с использованием криптовалют требует не просто точечных изменений, а комплексной модернизации всего арсенала уголовного права, процесса и криминалистики. Признание криптовалют имуществом – лишь фундамент. Над ним необходимо выстроить здание адекватных квалификационных подходов, эффективных следственных процедур, технологически оснащенных методов доказывания и конфискации, а также действенных международных механизмов сотрудничества.

Игнорирование специфики DeFi, смарт-контрактов и приватных активов создает опасные посылы для преступников. Успех возможен только через синергию права и технологий: внедрение ИИ в расследование, развитие блокчейн-криминалистики, обучение кадров и создание специализированной инфраструктуры для работы с цифровыми активами на всех стадиях – от изъятия до реализации. Промедление в решении этих вопросов не только снижает эффективность борьбы с уже существующими угрозами (вымогательством, мошенничеством, отмыванием коррупционных доходов), но и оставляет правовую систему неготовой к вызовам следующего технологического скачка, связанным с Web3, метавселенными и автономными экономическими агентами на блокчейне. Адаптация уголовно-правовой системы к цифровой реальности – это императив национальной безопасности и гарантия защиты прав граждан в новом технологическом измерении экономических отношений.

СПИСОК ИСТОЧНИКОВ

1. Долгиева, М. М. Противодействие легализации преступных доходов при использовании криптовалюты // Вестник Томского государственного университета. 2019. № 449. С. 213–218. DOI: 10.17223/15617793/449/26. EDN: NHAIRB.

2. Сидоренко, Э. Л. Правовой статус криптовалют в Российской Федерации // Экономика. Налоги. Право. 2018. Т. 11. № 2. С. 129–137. DOI: 10.26794/1999-849X-2018-11-2-129-137. EDN: YXKMKI.

3. Одинцов, С. В., Кошелюк Б. Е. Проблемы квалификации преступлений, сопряженных с использованием криптовалют // Вестник Томского государственного университета. 2023. № 487. С. 220–229. DOI: 10.17223/15617793/487/25. EDN: KEHEWG.

4. Ображиев, К. В. Хищение цифровой валюты (криптовалюты): проблемы квалификации // Уголовный закон в эпоху искусственного интеллекта и цифровизации : сборник трудов по материалам Всероссийской научно-практической конференции с международным участием в рамках I Саратовского международного юридического форума, посвященного 90-летнему юбилею Саратовской государственной юридической академии, Саратов, 9 июня 2021 года. Саратов : Саратовская государственная юридическая академия, 2021. С. 74–85.

5. Россинская, Е. Р., Рядовский И. А. Концепция вредоносных программ как способов совершения компьютерных преступлений: классификации и технологии противоправного использования // Всероссийский криминологический журнал. 2020. Т. 14. № 5. С. 699–709. DOI: 10.17150/2500-4255.2020.14(5).699-709. EDN: HNMPIX.

6. Колычева, А. Н., Васюков В. Ф. Отдельные аспекты противодействия использованию криптовалют в преступных целях // Криминалистика: вчера, сегодня, завтра. 2025. №. 1. С. 89–101. URL: https://kvsz.ru/ru/nauka/article/97208/view (дата обращения: 11.06.2025).

7. Русскевич, Е. А., Малыгин И. И. Преступления, связанные с обращением криптовалют: особенности квалификации // Право. Журнал Высшей школы экономики. 2021. № 3. С. 106–125. DOI: 10.17323/2072-8166.2021.3.106.125. EDN: SVTKLI.

8. Сидоренко, Э. Л. Defi-преступность: состояние, тенденции и криминологические модели // Russian Journal of Economics and Law. 2023. Т. 17. № 2. С. 327–341. DOI: 10.21202/2782-2923.2023.2.327-341.

9. Михайленко, Н. В., Рудин А. В. Арест криптовалют и цифровых финансовых активов: вызовы правового регулирования // Вестник Московского университета МВД России. 2024. № 5. URL: https://cyberleninka.ru/article/n/arest-kriptovalyut-i-tsifrovyh-finansovyh-aktivov-vyzovy-pravovogo-regulirovaniya (дата обращения: 11.05.2025).

10. Сатымбекова, К. Б., Касымов Н. М. Налогообложение операций с цифровой валютой (криптовалютой) в казахстанском законодательстве // Международные стандарты учета и аудита: ключевые изменения и нюансы перехода в условиях цифровой экономики : сборник статей Международной научно-практической конференции, Астана, 17 февраля 2023 года. Астана : Евразийский национальный университет им. Л. Н. Гумилева, 2023. С. 182-187. EDN: BKZUIH.

11. Цян, Ю., Харитонова Ю. С. Виртуальные валюты в праве Китая: от запрета криптовалют к цифровому юаню // Вестник Московского университета. Серия 11. Право. 2024. № 1. URL: https://cyberleninka.ru/article/n/virtualnye-valyuty-v-prave-kitaya-ot-zapreta-kriptovalyut-k-tsifrovomu-yuanyu (дата обращения: 11.05.2025).

12. Гаврилин, Ю. В., Бедеров И. С. Установление личности владельцев цифровой валюты: методологические основы // Труды Академии управления МВД России. 2021. № 4 (60). URL: https://cyberleninka.ru /article/n/ustanovlenie-lichnosti-vladeltsev-tsifrovoy-valyuty-metodologicheskie-osnovy (дата обращения: 11.05.2025).

13. Борануков, М. Х. Криптовалюта как предмет преступных посягательств против собственности (с примерами из судебной практики) // Научный портал МВД России. 2023. № 2 (62). URL: https://cyberleninka.ru/article/n/kriptovalyuta-kak-predmet-prestupnyh-posyagatelstv-protiv-sobstvennosti-s-primerami-iz-sudebnoy-praktiki (дата обращения: 11.05.2025).

14. Сидоренко, Э. Л. Право цифровых активов: учебник для бизнеса. М. : Юрлитинформ, 2025. 312 с.

REFERENCES

1. Dolgijeva M. M. Protivodejstvie legalizacii prestupnyh dohodov pri ispol'zovanii kriptovaljuty [Counteracting the legalization of criminal proceeds when using cryptocurrency]. Vestnik Tomskogo gosudarstvennogo universiteta – Vestnik Tomsk State University Journal. 2019, no. 449, pp. 213-218. (In Russ.).

2. Sidorenko E. L. Pravovoj status kriptovaljut v Rossijskoj Federacii [Legal status of cryptocurrencies in the Russian Federation]. Ekonomika. Nalogi. Pravo – Economics. Taxes. Law. 2018, vol. 11, no. 2, pp. 129-137. (In Russ.).

3. Odintsov S. V., Koshelyuk B. E. Problemy kvalifikacii prestuplenij, sopryazhennyh s ispol'zovaniem kriptovaljut [Problems of qualifying crimes associated with the use of cryptocurrencies]. Vestnik Tomskogo gosudarstvennogo universiteta – Tomsk State University Journal. 2023, no. 487, pp. 220-229. (In Russ.).

4. Obrazhiev K. V. [Theft of digital currency (cryptocurrency): issues of qualification]. Ugolovnyj zakon v epohu iskusstvennogo intellekta i cifrovizacii: sbornik trudov po materialam Vserossijskoj nauchno-prakticheskoj konferencii (Saratov, 9 June 2021) [Criminal Law in the Age of Artificial Intelligence and Digitalization: A Collection of Papers Based on the Materials of the All-Russian Scientific and Practical Conference with International Participation within the Framework of the First Saratov International Legal Forum, Dedicated to the 90th Anniversary of the Saratov State Law Academy]. Saratov: Saratov State Law Academy, 2021, pp. 74-85. (In Russ.).

5. Rossinskaya, E. R., Ryadovskij, I. A. Koncepciya vredonosnyh programm kak sposobov sovershenija komp'yuternyh prestuplenij: klassifikacii i tehnologii protivopravnogo ispol'zovaniya [The concept of malicious software as methods of committing computer crimes: classifications and illegal-use technologies]. Vserossijskij kriminologicheskij zhurnal – All-Russian Criminology Journal. 2020, vol. 14, no. 5, pp. 699-709. (In Russ.).

6. Kolycheva, A. N., Vasyukov, V. F. Otdel'nye aspekty protivodejstviya ispol'zovaniyu kriptovaljut v prestuplennyh celjah [Certain aspects of counteracting the use of cryptocurrencies for criminal purposes]. Kriminalistika: vchera, segodnya, zavtra – Forensics: yesterday, today, tomorrow. 2025, no. 1, pp. 89-101. (In Russ.).

7. Russkevich, E. A., Malygin, I. I. Prestupleniya, svyazannye s obrashcheniem kriptovaljut: osobennosti kvalifikacii [Crimes related to the circulation of cryptocurrencies: features of qualification]. Pravo. Zhurnal Vysshej shkoly ekonomiki – Law. Higher School of Economics Journal. 2021, no. 3, pp. 106-125. (In Russ.).

8. Sidorenko, E. L. DeFi-prestupnost': sostoyanie, tendencii i kriminologicheskie modeli [DeFi crime: state, trends and criminological models]. Russian Journal of Economics and Law. 2023, vol. 17, no. 2, pp. 327-341. (In Russ.).

9. Mikhajlenko, N. V., Rudin, A. V. Arest kriptovaljut i cifrovyh finansovyh aktivov: vyzovy pravovogo regulirovaniya [Seizure of cryptocurrencies and digital financial assets: challenges of legal regulation]. Vestnik Moskovskogo universiteta MVD Rossii – Vestnik in of Moscow University of the Ministry of Internal Affairs of Russia. 2024, no. 5. (In Russ.).

10. Satymbekova, K. B., Kasymov, N. M. [Taxation of digital-currency (cryptocurrency) transactions in Kazakhstan legislation]. Mezhdunarodnye standarty ucheta i

audita: klyuchevye izmeneniya i nyuansy perehoda v usloviyah cifrovoj ekonomiki: sbornik statej Mezhdunarodnoj nauchno-prakticheskoj konferencii (Astana, 17 February 2023) [International accounting and auditing standards: key changes and nuances of transition in the digital economy: a collection of articles from the International scientific and practical conference, Astana, February 17, 2023]. Astana: Evrazijskij nacional'nyj universitet im. L.N. Gumileva, 2023, pp. 182-187. (In Russ.).

11. Qian, Yu., Kharitonova Yu. S. Virtual'nye valjuty v prave Kitaja: ot zapreta kriptovaljut k cifrovomu juany [Virtual currencies in Chinese law: from the ban on cryptocurrencies to the digital yuan]. Vestnik Moskovskogo universiteta. Seriya 11. Pravo – Vestnik of Moscow University. Series 11. Law. 2024, no. 1. (In Russ.).

12. Gavrillin, Yu. V., Bederov, I. S. Ustanovlenie lichnosti vladel'cev cifrovoj valjuty: metodologicheskie osnovy [Identifying owners of digital currency: methodological foundations]. Trudy Akademii upravleniya MVD Rossii – Proceedings of the Academy of Management of the MIA of Russia. 2021, vol. 60, no. 4. (In Russ.).

13. Boranukov, M. H. Kriptovaljuta kak predmet prestupnyh posyagatel'stv protiv sobstvennosti (s primerami iz sudebnoj praktiki) [Cryptocurrency as an object of criminal offenses against property (with examples from judicial practice)]. Nauchnyj portal MVD Rossii – Scientific Portal of the MIA of Russia. 2023, vol. 62, no. 2. (In Russ.).

14. Sidorenko E.L. Pravo cifrovyh aktivov: uchebnik dlja biznesa [Digital asset law: a textbook for business]. Moscow: Yurlitinform, 2025, 312 p. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Перетолчин Артём Павлович, кандидат юридических наук, начальник кафедры административного права и административной деятельности ОВД. Восточно-Сибирский институт МВД России. 664074, Россия, г. Иркутск, ул. Лермонтова, д. 110.

INFORMATION ABOUT THE AUTHOR

Peretolchin Artem Pavlovich, Candidate of Legal Sciences, Head of the Department of Administrative Law and Administrative Activities of the Internal Affairs Directorate. East Siberian Institute of the Ministry of Internal Affairs of the Russian Federation. 110 Lermontov St., Irkutsk, Russia, 664074.

Статья поступила в редакцию 19.06.2025; одобрена после рецензирования 18.07.2025; принята к публикации 18.09.2025.

The article was submitted 19.06.2025; approved after reviewing 18.07.2025; accepted for publication 18.09.2025.