

Дата поступления рукописи в редакцию: 17.03.2026 г.
Дата принятия рукописи в печать: 30.04.2026 г.

DOI: 10.24412/2076-1503-2026-4-262-265

АВETИСЯН Борис Рафаелович,
Главный научный сотрудник
НИИ образования и науки,
e-mail: Boris.Avetisyan@gmail.com

АВETИСЯН Карэн Рафаелович,
Старший преподаватель
кафедры информационных технологий
и организации расследования киберпреступлений,
Московская академия Следственного комитета
Российской Федерации имени А.Я. Сухарева,
e-mail: Karen-Avetisyan-1989@bk.ru

ОСОБЕННОСТИ ОСУЩЕСТВЛЕНИЯ ПРОКУРОРСКОГО НАДЗОРА ЗА РАССЛЕДОВАНИЕМ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТЫ

Аннотация. Стремительное развитие технологий порождает принципиально новые вызовы для правоохранительных и надзорных органов. Криптовалюты, основанные на технологии блокчейн, создают беспрецедентные возможности для противоправной деятельности: отмывания денежных средств, финансирования терроризма, мошенничества и коррупции. Децентрализованная природа этих инструментов, их трансграничный характер и «псевдоанонимность» определяют традиционные методы расследования неэффективными.

Ключевые слова: прокурорский надзор, криптовалюта, противодействие преступлениям, анализ и корреляция.

AVETISYAN Boris Rafaelovich,
Chief Researcher at the Research Institute
of Education and Science

AVETISYAN Karen Rafaelovich,
Senior Lecturer, Department of Information Technology
and Cybercrime Investigation,
Moscow Academy of the Investigative Committee
of the Russian Federation named after A. Ya. Sukharev

FEATURES OF PROSECUTORIAL SUPERVISION FOR THE INVESTIGATION OF CRIMES COMMITTED USING CRYPTOCURRENCIES

Annotation. The rapid development of technology creates fundamentally new challenges for law enforcement and supervisory authorities. Cryptocurrencies based on blockchain technology create unprecedented opportunities for illegal activities: money laundering, terrorist financing, fraud and corruption. The decentralized nature of these tools, their cross-border nature, and their “pseudo anonymity” make traditional investigative methods ineffective.

Key words: prosecutor's supervision, cryptocurrency, crime prevention, analysis and correlation.

Правительство Российской Федерации и Всемирный экономический форум 13 октября 2021 года подписали меморандум о создании в России Центра четвертой промышленной революции. Это историческое событие определило траекторию цифровой трансформации нашей страны на десятилетия вперед. Ключевыми направлениями работы Центра стали: искусственный интеллект и интернет вещей, беспилотный транспорт, медицина и обработка больших данных.

Согласно меморандуму, Россия берет на себя роль одного из лидеров в формировании траектории технологических изменений. Московский Центр стал полигоном для инноваций - площадкой для тестирования правовых протоколов и экспериментальных правовых режимов, позволяющих безопасно внедрять технологии в промышленный и социальный секторы. Вхождение в глобальную сеть из 15 подобных центров обеспечило доступ к лучшим мировым практикам цифрового бизнеса. В стране уже насчитывается свыше 800 готовых IT-решений на базе ИИ, многие из которых представлены на международных рынках. Это создаёт основу для внедрения прорывных технологий, но одновременно требует адекватного правоприменения и межведомственного взаимодействия при противодействии преступным схемам.

ИИ-криминал становится всё более изощрённым: злоумышленники используют генеративные модели и машинное обучение для повышения эффективности атак. Исследование IBM/Resilience показывает, что ИИ ускорил традиционные схемы фишинга и социального инжиниринга, увеличив их успех примерно в 4–5 раз. Применение глубоких нейросетей позволяет киберпреступникам писать безупречно правдоподобные фишинговые сообщения и синтезировать голоса руководителей (deepfake), подрывая защиту через классические методы верификации.

Такие угрозы требуют от правоохранительных органов новых средств реагирования – машинного обучения для анализа трафика, поведенческого анализа и многофакторной аутентификации, помимо постоянного обучения персонала.

Цель настоящей статьи - систематизировать проблемы, с которыми сталкиваются оперативные работники, руководители и сотрудники прокуратуры при выявлении преступных систем, использующих криптовалюты, и предложить конкретные прикладные инструменты для совершенствования надзорной деятельности. Задачи исследования включают анализ судебной практики, выявление технологических уязвимостей и разработку методических рекомендаций по межведомственному взаимодействию.

Проблемы квалификации преступлений. Ключевыми проблемами остаются: отсутствие четкого правового статуса криптовалюты, анонимность транзакций, затрудняющая установление личности преступника, сложности доказывания умысла. Лица, совершающие противоправные деяния, используют сложные схемы, выглядящие как легальная инвестиционная деятельность.

Недостаток знаний о работе блокчейна и криптовалютных бирж у отдельных работников следственных органов и судов может приводить к ошибкам в квалификации преступлений. Необходима специализированная подготовка кадров и разработка методических рекомендаций по расследованию дел с использованием виртуальных активов.

Криптовалюта как объект правового регулирования. В сентябре 2023 года Мещанский суд Москвы вынес первый в России приговор по уголовному делу о хищении криптовалюты (дело WEX). Бывший системный администратор криптобиржи Алексей Иванов был признан виновным в совершении преступления, предусмотренного ч. 4 ст. 160 УК РФ (растрата в особо крупном размере). Суд установил, что фигурант присвоил вверенные ему криптовалюты и цифровые финансовые активы на сумму свыше 18 млрд рублей.

В соответствии с официальным отзывом Верховного Суда Российской Федерации от 17 декабря 2024 года (№ 10-ВС-6203/24), криптовалюта представляет собой цифровую форму актива, выпускаемую и регулируемую децентрализованной системой блокчейн с использованием криптографического шифрования. Судебная инстанция признала криптовалюту категорией имущества, в отношении которой действуют нормы уголовно-процессуального законодательства о наложении ареста и изъятии.

Правовое регулирование сферы виртуальных активов в Российской Федерации носит фрагментарный характер. Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте...» и Федеральный закон от 08.08.2024 № 223-ФЗ не выделяют криптовалюту как отдельную категорию ЦФА, не раскрывают полностью признаки и механизмы взаимодействия с ней. На территории Российской Федерации криптовалюта не является легальным платежным средством, однако не запрещена для обмена, накопления и инвестирования.

Верховный Суд Российской Федерации в ноябре 2025 года отменил взыскание с бывшего системного администратора, указав на необходимость пересмотра подходов к оценке ущерба в делах о криптовалютах. Это решение продемонстрировало сложности с квалификацией цифровых активов и определением их рыночной стоимости на момент совершения преступления.

Судебная практика показывает разнообразие квалификации преступлений с использованием криптовалют: мошенничество (ст. 159 УК РФ), организация финансовой пирамиды (ст. 172.2 УК РФ), легализация (отмывание) доходов (ст. 174, 174.1 УК РФ), хищение (ст. 158 УК РФ). Суды признают криптовалюту «иным имуществом», хищение которого образует состав преступления.

Зарубежный опыт правоприменения. Секретная служба США (USSS) за последнее десятилетие конфисковала цифровые активы на сумму почти 400 млн долларов. Глобальный центр следственных операций (GIOC) отслеживает средства, анализируя ончейн-данные с помощью инструментов с открытым исходным кодом. По состоянию на 2025 год правительство США контролирует около 198 тысяч биткоинов, накопленных через расследования - один из крупнейших биткоин-балансов в мире.

Компании Chainalysis, TRM Labs и Elliptic продают государствам инструменты анализа транзакций, строящие графы связей между кошельками, биржами и организациями. Только Chainalysis помогла правоохранительным органам по всему миру отследить и изъять криптоактивы более чем на 12 млрд долларов. Рынок криптоаналитики уже превышает 8-10 млрд долларов и растет двузначными темпами ежегодно.

В Китае Верховный народный суд признал юридическую силу доказательств на базе блокчейна. Интернет-суды принимают цифровые данные, собранные и хранимые в блокчейне с цифровыми подписями, надежными временными метками и верификацией значений хеш-функции. Этот опыт представляет значительный интерес для развития российской судебной практики.

Блокчейн-технология и механизм транзакций. Система блокчейн представляет собой распределенную базу данных последовательно связанных блоков, каждый из которых содержит информацию о предыдущем и последующем блоке. Каждая операция в сети получает уникальную хеш-сумму (ID транзакции) - 64-символьный hex-идентификатор, генерируемый автоматически и служащий глобальным аутентичным указателем на конкретную запись в реестре.

Транзакция следует рассматривать как сущность, включающую совокупность входных (vin) и выходных (vout) итераций - операций, фиксирующих поступление либо списание активов. Ключевыми атрибутами транзакции являются: txid (идентификатор транзакции), block_time (временная метка), value (сумма в сатоши), fee (комиссия), vin/vout (входы и выходы). Доказательство Меркла - последовательность значений хеш-функции - позволяет верифицировать подлинность каждой транзакции.

Типы криптокошельков и их криминалистическое значение. Центральным элементом взаимодействия с криптовалютой выступает криптокошелек - программное или аппаратное средство для генерации, хранения и управления криптографическими ключами. Публичный ключ (адрес кошелька) - буквенно-цифровая последовательность, аналог логина, доступная в открытом доступе. Приватный (закрытый) ключ - конфиденциальная последовательность символов, необходимая для подтверждения операций. Утрата приватного ключа равносильна потере всего содержимого кошелька.

Различают «холодные» (аппаратные) и «горячие» (программные) кошельки. Холодные кошельки затрудняют оперативный мониторинг в реальном времени и чаще используются для долгосрочного хранения. Горячие кошельки генерируют непрерывный массив следов, отражая высокую интенсивность операций и вовлеченность в совершение операций в режиме реального времени.

Список литературы:

[1] Федеральный закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» от 31.07.2020 N 259-ФЗ (последняя редакция) // СПС КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_358753/ (дата обращения: 20.02.2026).

[2] Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации» от 08.08.2024 N 223-ФЗ (последняя редакция) // СПС КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_482453/ (дата обращения: 20.02.2026).

[3] Федеральный закон «Об оперативно-розыскной деятельности» от 12.08.1995 № 144-ФЗ. // СПС КонсультантПлюс. URL: Федеральный закон «Об оперативно-розыскной деятельности» от 12.08.1995 № 144-ФЗ (дата обращения: 20.02.2026).

[4] Федеральный закон «О прокуратуре Российской Федерации» от 17.01.1992 № 2202-1. // СПС КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_262/ (дата обращения: 20.02.2026).

[5] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ. // СПС КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 20.02.2026).

[6] Отзыв Верховного Суда РФ от 17.12.2024 № 10-ВС-6203/24 // СПС КонсультантПлюс. URL: <https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=PRJ&n=259827#jbHrJGVN8ACgrQh5> (дата обращения: 20.02.2026).

[7] Доклад Генерального прокурора РФ на заседании Совета Федерации от 27.04.2025. // Rutube. URL: <https://rutube.ru/video/6ced6b144ec6cf5c48cc16ce04c862ad/> (дата обращения: 20.02.2026).

[8] ГОСТ 34.11-2018 «Информационная технология. Криптографическая защита информации». // НормативКонтур. URL: <https://normativ.kontur.ru/document?moduleId=9&documentId=377763> (дата обращения: 20.02.2026).

[9] ГОСТ Р 70462.1-2022 «Информационные технологии. Интеллект искусственный. Оценка робастности нейронных сетей. Часть 1. Обзор». // Электронный фонд правовых и нормативно-технических документов. URL: <https://docs.cntd.ru/document/1200193906> (дата обращения: 20.02.2026).

[10] ISO/IEC 10118-2:2010 Information technology - Security techniques - Hash-functions. // iso.org. URL: <https://www.iso.org/standard/44737.html> (дата обращения: 20.02.2026).

References:

[1] Federal Law “On Digital Financial Assets, Digital Currency, and Amendments to Certain Legislative Acts of the Russian Federation” dated July 31, 2020 N 259-FZ (latest revision) // SPS ConsultantPlus. URL: https://www.consultant.ru/document/cons_doc_LAW_358753/ (accessed: February 20, 2026).

[2] Federal Law “On Amendments to Certain Legislative Acts of the Russian Federation” dated August 8, 2024 N 223-FZ (latest revision) // SPS ConsultantPlus. URL: https://www.consultant.ru/document/cons_doc_LAW_482453/ (accessed: February 20, 2026).

[3] Federal Law “On Operational-Investigative Activities” of August 12, 1995, No. 144-FZ. // SPS

ConsultantPlus. URL: Federal Law “On Operational-Investigative Activities” of August 12, 1995, No. 144-FZ (accessed on February 20, 2026).

[4] Federal Law “On the Prosecutor’s Office of the Russian Federation” of January 17, 1992, No. 2202-I. // SPS ConsultantPlus. URL: https://www.consultant.ru/document/cons_doc_LAW_262/ (accessed on February 20, 2026).

[5] Criminal Procedure Code of the Russian Federation of December 18, 2001, No. 174-FZ. // SPS ConsultantPlus. URL: https://www.consultant.ru/document/cons_doc_LAW_34481/ (date accessed: 20.02.2026).

[6] Review of the Supreme Court of the Russian Federation dated 17.12.2024 No. 10-BC-6203/24 // SPS ConsultantPlus. URL: <https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=PR-J&n=259827#jbHrJGVN8ACgrQh5> (date accessed: 20.02.2026).

[7] Report of the Prosecutor General of the Russian Federation at the meeting of the Federation Council dated 27.04.2025. // Rutube. URL: <https://rutube.ru/video/6ced6b144ec6cf5c48cc16ce04c862ad/> (accessed: 20.02.2026).

[8] GOST 34.11-2018 “Information Technology. Cryptographic Protection of Information”. // NormativeKontur. URL: <https://normativ.kontur.ru/document?moduleId=9&documentId=377763> (accessed: 20.02.2026).

[9] GOST R 70462.1-2022 “Information Technology. Artificial Intelligence. Robustness Assessment of Neural Networks. Part 1. Review”. // Electronic Fund of Legal and Regulatory-Technical Documents. URL: <https://docs.cntd.ru/document/1200193906> (accessed: 20.02.2026).

[10] ISO/IEC 10118-2:2010 Information technology - Security techniques - Hash functions. // iso.org. URL: <https://www.iso.org/standard/44737.html> (accessed: 20.02.2026).



ЮРКОМПАНИ
www.law-books.ru

Юридическое издательство «ЮРКОМПАНИ»
издает научные журналы:

- Научно-правовой журнал «Образование и право», рекомендованный ВАК Министерства науки и высшего образования России (специальности 12.00.01, 12.00.02), выходит 1 раз в месяц.
- Научно-правовой журнал «Право и жизнь», рецензируемый (РИНЦ, E-Library), выходит 1 раз в 3 месяца.