УГОЛОВНОЕ ПРАВО И ПРОЦЕСС

Дата поступления рукописи в редакцию: 20.03.2026 г.
Дата принятия рукописи в печать: 30.04.2026 г.
DOI: 10.24412/2076-1503-2026-4-670-675

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

АВЕТИСЯН 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

ВЗАИМОДЕЙСТВИЯ ОРГАНОВ ВЛАСТИ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТЫ

Аннотация. *Действующим законодательством соблюдение прав и свобод человека при осуществлении ОРМ отнесено к предмету прокурорского надзора. Однако законодательно не определен процессуальный порядок рассмотрения судом ходатайств о проведении ОРМ, не предусмотрено участие прокурора в судебных заседаниях. Прокурор осуществляет надзор «постфактум», то есть уже после проведения оперативно-розыскных мероприятий, когда нарушения закона уже могут быть допущены. Отсутствие у граждан права обжалования состоявшихся судебных решений налагает на прокурора дополнительные обязанности гарантировать законность принятых решений.*

Ключевые слова: *прокурорский надзор, криптовалюта, противодействие преступлениям, взаимодействие.*

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

GOVERNMENT INTERACTIONS DURING THE INVESTIGATION OF INCIDENTS OF CRIMES COMMITTED USING CRYPTOCURRENCIES

Annotation. *By current legislation, the observance of human rights and freedoms in the implementation of MPas is attributed to the subject of prosecutorial supervision. However, the legislation does not define the procedural procedure for the consideration by the court of petitions for the conduct of an OPM, nor does it provide for the participation of the prosecutor in court sessions. The prosecutor supervises "after the fact", that is, after conducting operational investigative measures, when violations of the law may already have been committed. The lack of citizens' right to appeal court decisions imposes additional obligations on the prosecutor to ensure the legality of the decisions taken.*

Key words: *prosecutor's supervision, cryptocurrency, crime prevention, interaction.*

Прокурорский надзор за оперативно-розыскной деятельностью. Согласно докладу Генерального прокурора РФ на заседании Совета Федерации от 27 апреля 2025 года, количество нарушений законодательства об оперативно-розыскной деятельности в 2024 году возросло до 580 тысяч (на 2%). Прокурорский надзор за ОРД имеет свою специфику: оперативно-розыскная деятельность носит как гласный, так и негласный характер, организация и тактика ОРМ являются государственной тайной.

Межведомственное взаимодействие и информационная асимметрия. Система противодействия легализации (отмыванию) доходов в Российской Федерации сталкивается с рядом системных проблем: недостаточная координация между уполномоченными государственными органами, затрудненный обмен информацией, сложности в имплементации международных стандартов, низкая осведомленность участников рынка, технологические ограничения.

Информационная асимметрия выражается в недостаточной осведомленности участников рынка о требованиях законодательства в сфере ПОД/ФТ, что приводит к нарушениям и снижению эффективности системы в целом. Основную угрозу представляют организаторы преступных сетей - дропповоды, создающие нелегальную инфраструктуру для отмывания похищенных денег.

Росфинмониторинг разработал программный инструмент анализа криптовалютных транзакций «Прозрачный блокчейн», позволяющий видеть и анализировать операции с рядом криптовалют. Уже имеется несколько десятков уголовных дел, доведенных до суда, где такой анализ использовался. Однако потенциал инструмента недостаточно используется в межведомственном взаимодействии.

Международное сотрудничество. В марте 2026 года представители Генеральной прокуратуры РФ провели рабочие встречи с коллегами из стран СНГ, посвященные вопросам организации оборота цифровых валют и виртуальных активов. Экспертное совещание организовано совместно с Секретариатом Координационного совета генеральных прокуроров государств - участников СНГ.

Интерпол и Организация по безопасности и сотрудничеству в Европе организуют семинары, направленные на укрепление практических навыков судей и следователей в расследовании дел, связанных с криптоактивами. Учитывая трансграничный характер операций в криптовалюте, организация с глобальным охватом, такая как Интерпол, отлично подходит для оказания содействия при уголовном преследовании.

Ключевыми направлениями развития международного сотрудничества являются: заключение соглашений о взаимной правовой помощи, обеспечивающих оперативный обмен информацией; совместные операции с правоохранительными органами различных стран; участие в международных организациях по разработке стандартов; использование технологических инноваций для анализа транзакций.

Анонимность и децентрализация. Технологическая особенность криптовалюты, и используемой сеетвой инфраструктуры предоставляет возможность осуществлять финансирование по децентрализованной логистической форме вне «юрисдикции» регулятора. Природа таких транзакций - оперативность трансграничных переводов, «анонимность» операций - формирует цепочки теневых-серых зон для успешного проведения незаконных операций, в частности финансирования терроризма.

Для приватных или анонимных монет (Monero, Zcash) требуется дополнительный анализ смарт-контрактов и возможных миксеров. Криптовалютные микшеры (tumblers) позволяют запутать след транзакций, разбивая суммы на множество мелких переводов через различные адреса. Отследить обратный путь от зачисленных на банковскую карту денежных средств становится практически невозможным.

Основной риск криптовалют - анонимность владельца кошелька. Организации, обменивающие цифровую валюту (биржи и криптообменники), должны входить в правовое поле и выполнять обязанности по идентификации клиентов (KYC), сопоставимые с банковскими требованиями.

Доказывания в уголовном процессе. Использование результатов ОРД в качестве доказательств является весьма актуальной, поскольку ОРД лежит за рамками уголовного судопроизводства и на нее не распространяются его принципы. Результаты ОРД, чтобы стать доказательствами в уголовно-процессуальном смысле, должны быть дважды оценены с точки зрения допустимости.

На первом этапе прокурор оценивает допустимость результатов ОРД, на втором - допустимость сформированных на их основе доказательств. При выявлении недостатков в части оценки фактических данных и их преобразования в доказательства претензии следует предъявлять расследующему уголовное дело лицу, а не сотрудникам оперативного подразделения.

Доказательственное значение имеют публичные адреса и хеш-транзакции. Для установления связи криптоадреса с конкретным лицом требуется комплексный подход: анализ блок-

чейна, запросы к ПУВА, данные банковского комплаенса, результаты оперативно-технических мероприятий, компьютерно-технические экспертизы.

Блокчейн-аналитика. Практическая реализация анализа криптокошельков строится на открытых API блокчейн-обозревателей (Blockstream, Blockchair, Blockchain.com). Система запрашивает данные в формате JSON по адресу кошелька, автоматически определяя поддерживаемые валюты. Ключевые поля (txid, block_time, value, fee, prevout, is_coinbase) позволяют рассчитывать баланс, временные ряды, комиссию и роль кошелька в цепочке.

На основе этих данных формируется: общая статистика (входящие/исходящие суммы, время жизни кошелька, периоды простоя); топ-N взаимодействующих адресов по объему и частоте; граф связей с учетом «спреев» и «миксеров»; динамика баланса и фильтры по датам или токенам. Пользователь может перейти к анализу любого связанного адреса, строя итерационное древо транзакций.

Специализированные сервисы оценки рисков криптоактивов присваивают адресам условные уровни риска: низкий (до 35%), средний (35-75%), высокий (76-100%). Однако автоматическое присвоение риска носит вероятностный характер, и более высокая по качеству оценка возможна только при одновременном применении нескольких методов подтверждения.

Искусственный интеллект и нейросетевые технологии. Современные преступления с использованием криптовалют происходят в условиях массового шифрования трафика и децентрализованной инфраструктуры, где традиционные средства контроля теряют эффективность. Методы машинного обучения и нейросетевые технологии позволяют перейти от «реактивного» анализа к предиктивному, выявляя скрытые закономерности в паттернах активности криптокошельков.

Традиционные методы анализа трафика (DPI, сигнатурные правила Suricata/Snort) основаны на заранее заданных правилах и теряют работоспособность при шифровании (HTTPS, DoH/DoT/DoQ, VPN). Машинное обучение обучается непосредственно на данных и выявляет сложные закономерности без жесткого программирования правил.

Особую ценность представляют трансформеры и графовые нейронные сети с механизмом внимания (GAT). Трансформеры выявляют обфусцированный вредоносный код, многоэтапные атаки, DDoS и сканирование портов даже в зашифрованном трафике. GAT моделируют сеть как граф, где узлы - устройства, а ребра - связи с атрибутами. Гибридные архитектуры достигают F1 ≥ 0,99, значительно превосходя сигнатурные решения.

Поведенческий анализ и выявление паттернов. Поведенческий анализ пользователей начинается с формирования первичных сущностей по каждой цифровой платформе (социальные сети, мессенджеры, криптобиржи). Данные агрегируются из веб-логов, сессий, системных событий и кликовых карт, после чего проходят нормализацию, индексацию и каскадную сегментацию.

Процедуры обогащения и дообогащения позволяют выстраивать материнские и дочерние сущности: от уровня отдельного пользователя до сообществ и региональных хостингов. Результатом становится датасет паттернов активности, где каждая запись содержит последовательность действий, глубину взаимодействия и верифицирующие атрибуты.

Такой подход дает возможность прогнозировать негативные сценарии, включая переход средств через миксеры или аккумуляцию на горячих/холодных кошельках, с автоматическим обновлением статуса при мониторинге в фоновом режиме. Установление паттернов исследуемой категории инцидентов (следообразование в исследуемом контуре) является ключевым элементом криминалистического подхода.

На основании проведенного анализа проблем и существующей практики предлагаются следующие методические рекомендации по совершенствованию надзорной деятельности и взаимодействия органов власти в условиях цифровой трансформации.

Совершенствование прокурорского надзора. Необходимо разработать специализированные акты прокурорского реагирования, адаптированные для применения в рамках надзора за органами, осуществляющими ОРД. Существующие акты (протест, представление, предостережение) носят общенадзорный характер и не учитывают специфику оперативно-розыскной деятельности.

Необходимо развивать специальную подготовку прокурорских работников в области цифровых технологий, блокчейна и криптовалют. Прокуроры должны обладать компетенциями для оценки допустимости доказательств, полученных с использованием технических средств.

Организационные меры надзора:

- Создать в прокуратуре специализированные группы «Цифровой криминалистики» с доступом к Blockchair API.

- Ежегодные межведомственные тренинги (прокуратура + МВД + Росфинмониторинг) по ML-анализу.

- Мониторинг рисков: низкий/средний/высокий (сервисы типа Chainalysis-аналогов).

- Международное сотрудничество: через ЕАГ и Форум прокуроров СНГ (возврат активов).

Процессуальные механизмы. - Арест через изъятие приватных ключей + добровольную выдачу как условие досудебного соглашения (глава 40¹ УПК РФ).

- Обязательная компьютерно-техническая экспертиза + дактилоскопия устройств.

- Корреляция с ОТМ: геолокация, DPI-логи, VPN-цепочки.

- Единый протокол запросов к ПУВА и провайдерам (на базе документов) а именно:

- обязательные поля: Wallet ID, KYC (physical/legal), vin/vout с index, TXID1/TXID2, device fingerprint (IMEI/IMSI, IP gray/white, MAC, UUID, geolocation, browser, OS).

- шаблон запроса через Росфинмониторинг (закрытые каналы) + международные (ЕАГ, СНГ).

Укрепление межведомственного взаимодействия. Рекомендуется создать межведомственный центр анализа криптовалютных транзакций на базе Росфинмониторинга с участием представителей прокуратуры, Следственного комитета, МВД и ФСБ. Центр должен обеспечивать оперативный обмен данными и координацию действий при расследовании дел с использованием виртуальных активов.

Необходимо разработать единые стандарты запроса информации от провайдеров услуг виртуальных активов (ПУВА) и сетевых провайдеров. Запросы должны требовать предоставления полной цепочки идентификаторов - всех IP- и MAC-адресов, используемых портов, времени событий и применяемых протоколов на каждом участке.

Следует внедрить автоматизированные системы машинного соотнесения криптовалютных транзакций с фиатными операциями. Банки должны получать возможность сопоставлять зачисление средств на счет с датой, временем и суммой криптовалютной операции с учетом допустимого интервала и колебаний курса.

Развитие международного сотрудничества. Необходимо активизировать работу по заключению соглашений о взаимной правовой помощи с государствами, являющимися ключевыми юрисдикциями для криптовалютных бирж. Приоритетом должны стать страны, где зарегистрированы крупнейшие CEX-платформы.

Рекомендуется расширить участие российских правоохранительных органов в программах обучения Интерпола и ОБСЕ по расследованию дел с криптоактивами. Обмен опытом с зарубежными коллегами позволит адаптировать лучшие мировые практики к российским условиям.

Внедрение технологических решений. Предлагается масштабировать использование системы «Прозрачный блокчейн» на все территориальные органы Росфинмониторинга и обеспечить доступ к ней следователей и прокуроров. Необходимо разработать методические рекомендации по использованию результатов анализа в качестве доказательств в уголовном процессе.

Следует создать центры компетенций по блокчейн-аналитике в структуре крупнейших следственных управлений. Центры должны оснащаться программными комплексами анализа транзакций и обучать специалистов работе с инструментами Chainalysis, TRM Labs или их отечественными аналогами.

Рекомендуется разработать стандарты использования искусственного интеллекта в правоохранительной деятельности, включая требования к прозрачности алгоритмов, обязательности человеческого контроля за финальными решениями и проведению аудита на дискриминационные смещения перед вводом систем в эксплуатацию.

Технические инструменты анализа (открытые API + ИИ):

- Blockchair/Blockstream API: JSON-структуры с txid, vin/vout, value, block_time. Автоматическое построение графов связей (центральный узел — исследуемый адрес).

- Merkle proof + backpropagation (как в нейросетях): для цепочек транзакций.

- Графовые нейронные сети (GAT) и трансформеры: выявление аномалий (мик-серы, спреи). Метрика F1-score ≥ 0,99.

- Интеграция с отечественными решениями (более 800 ИИ-продуктов РФ по 4IR).

Здоровье нации как метафора: Как врач диагностирует рак по биомаркерам, так прокурорский надзор должен выявлять «метастазы» крипто-пирамид и коррупции через цифровые биомаркеры (UTXO, паттерны трафика). 4IR даёт нам «вакцину» — ИИ и блокчейн-аналитику.

Выводы. Четвёртая промышленная революция, стартовавшая в 2021 году, сделала крипто-валюту не угрозой, а вызовом, который мы обязаны обратить в преимущество. Предлагаемые тезисы и инструменты позволят Генеральной прокуратуре не только эффективно надзирать за оперативными органами, но и формировать доказательственную базу, минимизировать ущерб и возвращать активы. Готов представить полные методические рекомендации, включая алгоритмы API-запросов и шаблоны протоколов.

Проведенное исследование позволяет сформулировать следующие выводы.

Во-первых, четвертая промышленная революция, обозначенная в меморандуме ВЭФ 2021

года, создает беспрецедентные вызовы для правоохранительных и надзорных органов. Криптовалюты, искусственный интеллект и интернет вещей трансформируют как способы совершения преступлений, так и методы их расследования.

Во-вторых, существующая система прокурорского надзора за оперативно-розыскной деятельностью имеет значительные пробелы, связанные с отсутствием специализированных актов реагирования, постфактум характером надзора и недостаточной технической подготовкой кадров. Необходима адаптация надзорных механизмов к условиям цифровой экономики.

В-третьих, межведомственное взаимодействие в сфере противодействия отмыванию доходов сталкивается с информационной асимметрией, недостаточной координацией и технологическими ограничениями. Создание межведомственного центра анализа криптовалютных транзакций позволит преодолеть эти барьеры.

В-четвертых, технологические решения на базе искусственного интеллекта и нейросетей открывают новые возможности для анализа паттернов активности и выявления преступных схем. Гибридные архитектуры машинного обучения достигают точности F1 ≥ 0,99, значительно превосходя традиционные сигнатурные методы.

В-пятых, развитие международного сотрудничества является критически важным фактором успеха, учитывая трансграничный характер криптовалютных операций. Участие в программах Интерпола и обмен опытом с зарубежными коллегами позволят адаптировать лучшие мировые практики.

Реализация предложенных методических рекомендаций позволит органам прокуратуры эффективнее осуществлять надзорную деятельность в отношении оперативных органов и органов контроля при выявлении преступных схем с использованием криптовалют. Современный инструментарий анализа и оценки, основанный на технологиях ИИ и блокчейн-аналитике, станет надежным орудием в борьбе с цифровой преступностью.

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-I. // 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 Con-

sultantPlus. 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=PRJ&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).