Анна Михайловна ЧИХРАДЗЕ,
кандидат юридических наук, ORCID 0009-0000-0763-2228
Санкт-Петербургский университет МВД России (г. Санкт-Петербург)
доцент кафедры криминалистики
anna.chikhradze@mail.ru

Научная статья
УДК 343.98.067[343.985.7:004.6]

БЛОКЧЕЙН-АНАЛИТИКА КАК НЕПРОЦЕССУАЛЬНАЯ ФОРМА ИСПОЛЬЗОВАНИЯ СПЕЦИАЛЬНЫХ ЗНАНИЙ

КЛЮЧЕВЫЕ СЛОВА. Расследование преступлений, цифровая преступность, криптовалюта, блокчейн-аналитика, распределенный реестр данных, специализированный программный продукт, специальные знания.

АННОТАЦИЯ. ***Введение***. *Блокчейн-аналитика рассматривается в статье как непроцессуальная форма использования специальных знаний в контексте раскрытия и расследования преступлений, совершенных с использованием криптовалютных активов. Актуальность темы проведенного автором исследования обусловлена ростом показателей цифровой преступности, а также необходимостью адаптации криминалистических методов к особенностям функционирования распределенных реестров данных.* ***Методы***. *В ходе исследования были востребованы общенаучные и специальные методы. Логико-структурный метод применялся для изучения блокчейн-аналитики как непроцессуальной формы использования специальных знаний. Формально-юридический метод позволил проанализировать законодательные нормы в качестве оснований для внедрения высокотехнологичных программных решений в правоохранительную деятельность.* ***Результаты***. *Определена роль блокчейн-аналитики как особой непроцессуальной формы использования специальных знаний в рамках раскрытия и расследования преступлений, совершаемых с использованием криптовалюты. Особое внимание уделено специализированным программным продуктам, осуществляющим блокчейн-аналитику в режиме реального времени, таким как «Chainalysis», «Crystal Blockchain», «Elliptic», а также отечественной системе «Прозрачный блокчейн». Обозначены этапы аналитической работы, источники информации, механизм выявления транзакций повышенного риска. Сделан вывод о необходимости закрепления процедуры и результатов блокчейн-аналитики в частной методике расследования как эффективного элемента современной цифровой криминалистики.*

ВВЕДЕНИЕ

Развитие цифровых технологий в последние годы привело к существенному увеличению числа преступлений, совершаемых в виртуальном пространстве. В условиях цифровизации блокчейн-технологии и связанные с ними криптовалюты приобретают всё большее значение в криминалистической практике, в том числе в связи с особенностями расследования преступлений, совершенных с их использованием. Вследствие анонимности транзакций криптовалюты активно используются для легализации преступных доходов и финансирования преступной деятельности, что обусловливает необходимость использования специальных знаний для эффективного расследования таких преступлений.

Как неоднократно отмечалось в криминалистической науке, цифровые доказательства приобретают ключевое значение в расследовании преступлений, совершенных в цифровой среде, что требует применения новых подходов и развития аналитических методов [1, с. 398]. Поскольку специфика криптовалюты и распределенных реестров данных, а также функционирование криптоэкосистемы в целом создают определенного рода сложности в расследовании вышеназванных общественно опасных деяний, именно блокчейн-аналитика становится крайне актуальной как инно-

Anna M. CHIKHRADZE,
Cand. Sci. (Jurisprudence), ORCID 0009-0000-0763-2228
Saint Petersburg University of the Ministry of
the Interior of Russia (Saint Petersburg, Russia)
Associate Professor of the Department of Criminalistics
anna.chikhradze@mail.ru

BLOCKCHAIN ANALYTICS AS A NON-PROCEDURAL FORM OF USING SPECIALIZED KNOWLEDGE

KEYWORDS. Crime investigation, digital crime, cryptocurrency, blockchain analytics, distributed data registry, specialized software product, specialized knowledge.

ANNOTATION. ***Introduction***. *Blockchain analytics is considered in the article as a non-procedural form of using specialized knowledge in the context of solving and investigating crimes committed using cryptocurrency assets. The relevance of the topic of the study conducted by the author is due to the growth of digital crime rates, as well as the need to adapt forensic methods to the features of the functioning of distributed data registries.* ***Methods***. *The study required general scientific and special methods. The logical-structural method was used to study blockchain analytics as a non-procedural form of using specialized knowledge. The formal-legal method made it possible to analyze legislative norms as grounds for the introduction of high-tech software solutions in law enforcement.* ***Results***. *The role of blockchain analytics is determined as a special non-procedural form of using specialized knowledge in the context of solving and investigating crimes committed using cryptocurrency. Particular attention is paid to specialized software products that perform blockchain analytics in real time, such as «Chainalysis», «Crystal Blockchain», «Elliptic», as well as the domestic system «Transparent Blockchain». The stages of analytical work, sources of information, and the mechanism for identifying high-risk transactions are outlined. A conclusion is made about the need to consolidate the procedure and results of blockchain analytics in a private investigation methodology as an effective element of modern digital forensics.*

вационная методика анализа цифровых следов в особых случаях, которые законом могут быть даже не предусмотрены [2, с. 70; 3, с. 309; 4 с. 338].

Теоретической основой проведенного нами исследования стали труды в области цифровой криминалистики и материалы практики использования специализированных IT-решений при расследовании и раскрытии преступлений, совершаемых с использованием криптовалют. Как подчеркивается в научной литературе, анализ цифровых следов – от выявления закономерностей их возникновения и до интерпретации – является методологической основой блокчейн-аналитики [5, с. 257; 6, с. 126]. Последняя выступает непроцессуальной формой применения специальных знаний, ее основная задача – идентификация и трассировка субъектов противоправной деятельности. Однако псевдоанонимность распределенных реестров серьезно затрудняет установление связи криптовалютных адресов с фигурантами, что и предопределяет необходимость привлечения специализированных инструментов блокчейн-аналитики для преодоления данного барьера [7].

Аналитическая обработка криминалистически значимой информации представляет собой объединение разрозненных информационных блоков для получения новых знаний, которые в дальнейшем могут быть использованы при расследовании преступлений [8, с. 151]. Подобный подход отражен и в трудах Р.Р. Карданова и А.А. Курина, где аналитическая обработка рассматривается как структурирование и системная интерпретация фрагментарных цифровых данных в целях формирования криминалистически значимой информации [9, с. 174]. При этом стоит отметить, что подобного рода деятельность представляется невозможной без лиц, обладающих специальными знаниями в сфере блокчейн-аналитики (например специалистов Росфинмониторинга) [10, с. 670].

Целями нашего исследования были определение возможностей и оценка значения блокчейн-аналитики как одной из наиболее эффективных непроцессуальных форм использования специальных знаний в раскрытии и расследовании преступлений, совершенных с использованием криптовалюты.

МЕТОДЫ

Методологическую основу исследования, результаты которого представлены в настоящей статье, составили общенаучные и специальные методы научного познания. Логико-структурный метод был востребован при анализе блокчейн-аналитики как непроцессуальной формы использования специальных знаний. Формально-юридический метод применен для анализа законодательных норм как основания использования программных решений в правоохранительной деятельности. Эмпирическая база исследования была сформирована на основе изучения научных публикаций, открытых данных правоохранительных органов, аналитических отчетов.

РЕЗУЛЬТАТЫ

Блокчейн-аналитика представляет собой специфический метод исследования, который

предполагает анализ транзакций в распределенных реестрах данных, применяемый в контексте расследования преступлений, совершенных с использованием криптовалюты. Этот метод получения криминалистически значимой информации не носит процессуального характера, поскольку реализуется вне предусмотренных УПК РФ следственных действий. Однако он позволяет оперативно выявлять скрытые финансовые связи, структуру преступных сообществ и каналы финансирования незаконной деятельности.

Усиление практической потребности в его использовании обусловлено усложнением процессов выявления, фиксации и сбора цифровых доказательств, а также необходимостью анализа значительного массива данных блокчейна, что вызывает потребность применения специальных технических средств и программного обеспечения, позволяющих эффективно извлекать и анализировать данные цифровых платформ [11, с. 357]. По данным «RAND Corporation», опубликованным в 2022 году, более 80% опрошенных сотрудников правоохранительных органов США считают блокчейн-анализ крайне актуальным источником данных при расследовании преступлений, связанных с криптовалютой[1].

Сегодня сложно представить эффективную блокчейн-аналитику, осуществляемую сведущими лицами, без специализированных программных ресурсов, поскольку охват технологических особенностей функционирования блокчейна, а также значительных массивов данных, подлежащих анализу, находится за рамками человеческих возможностей. Специализированное программное обеспечение позволяет идентифицировать участников транзакций, несмотря на высокий уровень анонимности. Использование цифровых аналитических инструментов значительно повышает эффективность мероприятий правоохранительных органов в сфере противодействия преступлениям, совершаемым с использованием криптовалют. К числу таких программ относятся «Chainalysis»[2], «Elliptic»[3], «Titanium»[4], «Crystal»[5] и ряд других[6]. Есть немало примеров успешной работы аналитиков, использовавших названные программные продукты, которая позволила привлечь виновных к уголовной ответственности. Приведем лишь два из них. Так, в марте 2025 года данные, собранные аналитиками компании «Elliptic», помогли Секретной службе США[7] раскрыть деятельность криптовалютной биржи «Garantex», связанной с отмыванием денежных средств на сумму 96 миллиардов долларов, полученных от даркнет-рынков, в результате вымогательства с использованием компьютерных программ и хакерских атак. Кластеризационные эвристики «Elliptic» обеспечили возможность установить взаимосвязь между адресами биржи и фигурантами дела, идентифицировать лиц, осуществлявших противоправную деятельность с использованием криптовалютных кошельков как средства совершения преступления[8]. Другим показательным примером является ликвидация крупного нелегального маркетплейса «Hydra» при аналитической поддержке расследования со стороны компании «Crystal Blockchain». Ее специалисты, применив программные инструменты, отследили вывод криптовалюты через «Bitcoin Bank Mixer»[9], определили конечные кошельки и биржевые выходы, что позволило следователям Федерального криминального ведомства Германии идентифицировать виновных, изъять серверы «Hydra» и конфисковать биткоины на сумму свыше выше 25 миллионов евро[10].

Таким образом, мировой опыт убедительно показывает: без комплексных программно-аналитических платформ эффективная трассировка криптовалютных транзакций невозможна. Этот превалирующий фактор объективно потребовал создания отечественного программного решения, сопоставимого по функциональным возможностям с вышеназванными инструментами блокчейн-аналитики. Именно эту роль призван выполнять разработанный Росфинмониторингом программный комплекс «Прозрачный блокчейн», предназначенный для аналитического сопровождения расследований в распределенных реестрах данных [12, с. 139.]. Правовыми основаниями создания данного инструмента являются поручение Президента Российской Федерации В.В. Путина от 29 октября 2021 г. Пр-2061 и протокол заседания Государственного антинаркотического комитета от 25 июня 2021 г. № 48.

В рамках выполнения основных своих задач «Прозрачный блокчейн» позволяет выявлять и

[1] Merkle Science. Strategies for law enforcement to identify and investigate crypto crimes // URL: https://www.merklescience.com/strategies-for-law-enforcement-to-identify-and-investigate-crypto-crimes (дата обращения: 05.04.2025).
[2] Chainalysis: blockchain data platform // URL: https://www.chainalysis.com/ (дата обращения: 20.04.2025).
[3] Elliptic: blockchain analytics & crypto compliance solutions // URL: https://www.elliptic.co/ (дата обращения: 20.04.2025).
[4] TITANIUM Project (Tools for the Investigation of Transactions in Underground Markets) // URL: https://www.titanium-project.eu/ (дата обращения: 20.04.2025).
[5] Crystal Intelligence: blockchain analytics & forensic solutions // URL: https://crystalintelligence.com/ (дата обращения: 20.04.2025).
[6] Пинская Т.В., Смольянинов Е.С. Международный опыт противодействия преступной деятельности с использованием криптовалют: Учебно-практическое пособие. М.: Академия управления МВД России, 2021. С. 54.
[7] United States Secret Service: official website // URL: https://www.secretservice.gov/ (дата обращения: 20.04.2025).
[8] Elliptic data used by US Secret Service in investigation into $96 billion Russian crypto exchange Garantex // URL: https://www.elliptic.co/media-center/elliptic-data-used-by-us-secret-service-in-investigation-into-60-billion-russian-crypto-exchange-garantex (дата обращения: 02.04.2025).
[9] Bitcoin Bank Mixer: illicit service laundering Hydra Market proceeds // URL: https://www.chainalysis.com/blog/bitcoin-bank-mixer-hydra (дата обращения: 20.04.2025).
[10] Illegale Darknet-Plattform «Hydra Market» abgeschaltet // URL: https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2022/Presse2022/220405_PM_IllegalerDarknetMarktplatz.html (дата обращения: 20.04.2025).

фиксировать криптовалютные транзакции в распределенном реестре, идентифицировать криптовалютные кошельки и их владельцев, а также прогнозировать потенциальные преступные схемы на основе данных блокчейна и выявленных моделей поведения.

Инициация процесса осуществления анализа такого типа производится уполномоченным аналитиком Росфинмониторинга в силу:

1) запроса, поступившего от правоохранительных органов (органов государственной власти). Такой запрос должен содержать в себе ряд обязательных элементов:

- описание характера противоправной деятельности;
- указание на период времени, в течение которого, по версии следствия, совершались преступные действия;
- обоснование связи расследуемого преступления с легализацией преступных доходов, указание на возможные способы легализации;
- указание на размер ущерба либо предполагаемого преступного дохода;
- идентификационные данные фигурантов (фамилии, имена, отчества, ИНН, даты рождения, адреса регистрации);
- обоснование связей между фигурантами в противоправной деятельности и их ролей;

2) результатов первичной проверки по базам данных Росфинмониторинга без направления запросов в кредитные и иные организации в 30-дневный срок, применяемой к конкретным лицам либо адресам в рамках ст. 6 Федерального закона от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», или поручения правоохранительных органов (до направления запросов в банки, налоговые и другие организации);

3) материалов финансового расследования, проводимого по собственной инициативе ведомства на основании подп. «д» п. 4 ст. 6 Федерального закона от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», а также приказа Федеральной службы по финансовому мониторингу от 8 февраля 2022 г. № 18 «Об утверждении Особенностей представления в Федеральную службу по финансовому мониторингу информации, предусмотренной Федеральным законом от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»» в отношении конкретных физических или юридических лиц (их криптоадресов), когда внутренние идентификаторы или внешние сигналы показывают высокий риск участия таких субъектов в противоправной деятельности. Цель расследования – собрать и подготовить аналитический отчет (по форме ФТМ-2) для последующей передачи в правоохранительные органы для возбуждения уголовного дела;

4) материалов углубленного финансового расследования. Это проверка с направлением запросов в кредитные организации, налоговые органы, органы ГИБДД, реестры объектов недвижимости. Срок ее проведения составляет 6 месяцев. Проверка такого рода осуществляется в отношении тех же лиц и структур, что и в случаях, описанных выше, Управлением финансовых расследований Росфинмониторинга (центральный аппарат) совместно с его территориальными органами, при необходимости привлекаются специалисты МВД, СК, ФСБ, Банка России.

Работа аналитиков в программном комплексе «Прозрачный блокчейн» проводится в несколько этапов:

1) предпроверочный анализ, который включает в себя:

- сбор данных об искомых объектах – поиск и отбор информации из различных источников (on-chain идентификаторы, off-chain данные, реестры государственных органов, OSINT-источники);
- обработку информации – анализ, систематизация и структурирование полученных данных с целью их последующего накопления и интеграции с другими информационными ресурсами;
- накопление обработанных и структурированных собранных сведений, образующих аналитическую информацию;
- анализ информации – разрешается вопрос о наличии или отсутствии оснований для дальнейшего расследования;

2) первичная проверка – уточнение и проверка информации через доступные ресурсы без официальных запросов;

3) углубленное финансовое расследование – сбор дополнительных данных посредством направления официальных запросов в органы власти, кредитные организации, проведение глубокого анализа полученных сведений;

4) реализация результатов – передача материалов в форме аналитического отчета (ФТМ-2/ФТМ-3) в правоохранительные органы для дальнейшего возбуждения уголовного дела либо производства следственных действий;

5) сопровождение переданных материалов – контроль и информационное сопровождение взаимодействия с уполномоченными органами.

Аналитический процесс можно описать в виде трехзвенной системы: поступление данных в единое хранилище; их аналитическая обработка, под которой понимается формирование реестров, поведенческих моделей, стратегический и оперативный анализ; передача результатов аналитики в компетентные органы либо в те структуры, которые направили запрос (правоохранительные органы, ФНС, Банк России и др.).

При мониторинге операций с виртуальными активами и отслеживании криптовалютных потоков необходимо учитывать специфику области применения «Прозрачного блокчейна». Мониторинг транзакционной активности включает в себя пять последовательных этапов:

1) мониторинг криптовалютных адресов фигурантов для выявления подозрительных транзакций в режиме реального времени. Под мониторингом адресов следует понимать постоянное автоматизированное наблюдение за транзакциями

в распределенном реестре данных в целях своевременного выявления операций, перечисленных в ст.ст. 6, 7 Федерального закона от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», а также Приказом Росфинмониторинга «Об утверждении Особенностей представления в Федеральную службу по финансовому мониторингу информации, предусмотренной Федеральным законом от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»», которые могут быть связаны с противоправной деятельностью (превышение лимита суммы, множественные транзакции с одного адреса, связь с ранее промаркированными подозрительными адресами). Такие операции подпадают под определенные алгоритмические и аналитические критерии в рамках кластерного анализа;

2) составление аналитических отчетов. Получив данные путем мониторинга программа автоматически либо с помощью аналитика формирует специализированный аналитический отчет, который представляет собой документ установленной формы, отражающий ключевые факты и выводы по результатам исследования. В отчете приводится информация о транзакциях, участниках операций, описываются риски и потенциальные связи с нелегальной деятельностью, что позволяет правоохранительным органам оперативно реагировать и принимать необходимые процессуальные решения;

3) исследование цепочки связей – определение всех возможных участников транзакций. «Прозрачный блокчейн» имеет такую возможность благодаря использованию специализированных алгоритмов. В результате их работы формируется подробная схема транзакций с указанием их участников, выявляется взаимодействие с иными субъектами, например биржами и банками, что предоставляет возможность отследить полный маршрут движения виртуальных валют;

4) контроль адресов – одна из наиболее полезных функций, которая подразумевает под собой своеобразную «маркировку» адресов. На данном этапе ведется автоматизированный учет адресов, которые ранее вовлекались в подозрительные либо преступные транзакции, с автоматическим же уведомлением аналитиков о любых действиях, совершенных с использованием таких адресов. Именно автоматизация контроля и уведомления аналитиков отличает специализированное программное обеспечение от иных сервисов учета, таких как КОСАтка[1] и др.;

5) определение принадлежности адресов биржам/субъектам. Отслеживание связи между анонимными адресами, обменниками и криптовалютными биржами является одним из важнейших направлений аналитической работы, поскольку установление таких связей значительно повышает шансы деанонимизации пользователей, а также создает необходимые условия для того, чтобы правоохранительные органы получили информацию для подготовки официальных запросов на раскрытие данных клиентов криптовалютных сервисов в рамках расследования;

6) составление и применение черных списков баз данных адресов, которые были уличены в противоправной деятельности. Использование таких списков позволяет мгновенно выявлять и блокировать транзакции, поступающие с подозрительных адресов. Система «Прозрачный блокчейн» автоматически сравнивает входящие данные с адресами, внесенными в черные списки, и сигнализирует о наличии потенциальной угрозы, что минимизирует риски пропуска подозрительных транзакций;

7) составление баз данных адресов. Эффективность аналитической работы зависит во многом от качества имеющегося массива информации, а также ее актуальности. Именно поэтому создание и регулярное обновление специализированных баз данных являются ключевыми элементами работы «Прозрачного блокчейна». На сегодняшний день программа имеет более 255 внутренних специализированных реестров (например: дела финансовых расследований, мероприятия, фигуранты проверок, запросы правоохранительных органов, запросы иностранных подразделений финансовых разведок), основанных более чем на 2200 классифицирующих признаках. Эти базы данных содержат различные сведения об отслеживаемых транзакциях – время, частота операций и др.;

8) эффективность аналитической деятельности тесно связана с наглядностью предоставления информации, то есть с визуализацией связей, в особенности тогда, когда речь идет о специфической группе преступлений, совершаемых с использованием криптовалют. Интерактивная визуализация финансовых потоков, использования криптовалютных миксеров, связей между адресами и субъектами позволяет аналитикам и компетентным органам быстро ориентироваться в больших массивах данных, выявлять ключевые элементы преступных схем и делать обоснованные выводы о роли и степени вовлеченности в них тех или иных конкретных лиц.

В связи с этим важно подчеркнуть, что анализ блокчейна проводится с использованием программных комплексов и интернет-ресурсов [13, с. 68-69], без этого идентификация участников транзакций невозможна. Проанализировав основные направления деятельности отечественного программного продукта «Прозрачный блокчейн», мы пришли к выводу о том, что он сегодня играет важную роль в повышении эффективности аналитической работы в контексте расследования преступлений, совершаемых с использованием криптовалюты, позволяя решать идентификационные и диагностические задачи в условиях финансовых расследований [14, с. 190].

Следует отметить, что, несмотря на столь высокий уровень технической и правовой значимости, блокчейн-аналитику в настоящее время можно отнести исключительно к числу непроцессуальных форм использования специальных знаний. Это

[1] КОСАтка – российская платформа, предназначенная для предупреждения и расследования преступлений, связанных с оборотом цифровых финансовых активов.

обстоятельство обусловлено тем, что, во-первых, она осуществляется вне рамок процессуальной деятельности, то есть не сопряжена с производством следственных либо иных процессуальных действий, а выполняется в рамках межведомственного сотрудничества. Во-вторых, ее результаты представляют собой предварительный экспертно-аналитический материал. На его основе выстраиваются версии, разрабатываются оперативные мероприятия и подготавливаются основания для возбуждения уголовного дела или проведения следственных действий, предусмотренных в УПК РФ. Ведь, как справедливо отмечается в научной литературе, к непроцессуальным формам использования специальных знаний могут быть причислены «предварительные (доэкспертные) исследования, ведомственные расследования, справочно-консультационная деятельность специалистов» [15, с. 204], что полностью соотносится с существующей практикой блокчейн-аналитики. В-третьих, обязательного привлечения лица в качестве специалиста в рамках конкретного уголовного дела блокчейн-аналитика не требует, в ряде случаев она осуществляется в инициативном порядке. Все эти аспекты позволяют отнести блокчейн-аналитику к категории непроцессуальных форм использования специальных знаний, обладающих высокой информационной ценностью.

ЗАКЛЮЧЕНИЕ

Результаты проведенного нами исследования дают основания констатировать, что блокчейн-аналитика представляет собой особую самостоятельную непроцессуальную форму применения специальных знаний при раскрытии и расследовании преступлений, совершенных с использованием криптовалюты. Ее основной задачей является анализ транзакций в распределенных реестрах данных для выявления связей между субъектами с целью их последующей идентификации. Специализированные программные продукты при выполнении аналитических задач позволяют не только выявлять подозрительные транзакции и отслеживать активность криптовалютных кошельков, но и устанавливать связи между анонимными адресами и реальными субъектами, что существенно расширяет возможности правоохранительных органов в условиях цифровизации преступной деятельности.

В результате анализа практики использования отечественного программного инструмента «Прозрачный блокчейн» мы пришли к заключению о том, что в контексте расследования криптовалютных преступлений блокчейн-аналитика активно используется уполномоченными специалистами Росфинмониторинга, а также сотрудниками следственных и оперативных подразделений МВД России. Интеграция «Прозрачного блокчейна» в межведомственную информационно-аналитическую инфраструктуру органов финансового контроля и правоохранительных органов демонстрирует высокую степень адаптации технологий к потребностям национальной правоприменительной практики. Есть все основания говорить о том, что сегодня блокчейн-аналитика является одном из ключевых инструментов цифровой криминалистики, формируя базу для эффективного межведомственного взаимодействия, а также создавая предпосылки для повышения раскрываемости преступлений, совершенных с использованием криптовалюты, и укрепления правопорядка в условиях развития новых финансовых технологий. ■

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Лобачёв Л.Л., Куцаков Ф.В. Цифровая криминалистика: возможности и перспективы развития // Вопросы студенческой науки. 2022. № 12 (76). С. 398-400.

2. Челышева О.В. Непроцессуальные формы использования специальных знаний при расследовании преступлений // Мир юридической науки. 2016. № 1-2. С. 70-76.

3. Зайцев А.А., Сулаева Д.С. Криптовалюта как элемент криминалистической характеристики преступлений // Проблемы правовой и технической защиты информации. 2021. № 9. С. 309-310.

4. Самойло В.А. Характерные особенности преступлений, связанных с использованием криптовалют // Преступность в СНГ: проблемы предупреждения и раскрытия преступлений. Сборник материалов конференции. В 3 ч. Воронеж, 2023. Ч. 1. С. 337-338.

5. Расторопов С.В. Цифровые доказательства в расследовании преступлений // Пробелы в российском законодательстве. 2020. Т. 13. № 5. С. 256-259.

6. Курин А.А. Совершенствование системы информационного обеспечения раскрытия и расследования преступлений // Альманах-2018. Волгоград, 2018. С. 126-135.

7. Atlam H.F., Ekuri N., Azad M.A., Lallie H.S. Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions // Electronics. 2024. Vol. 13. № 17. Art. 3568.

8. Ланцова А.В., Хаснутдинов Р.Р. Проблематика виртуального следа в цифровой криминалистике // International Journal of Humanities and Natural Sciences. 2020. Т. 12-3 (51). С. 149-151.

9. Карданов Р.Р., Курин А.А. Аналитическая обработка криминалистически значимой информации // Вестник Восточно-Сибирского института МВД России. 2019. № 2 (89). С. 173-177.

10. Гармаев Ю.П., Осипов Г.П. Привлечение специалиста для исследования криптовалют в уголовном, гражданском и арбитражном судопроизводствах // Вестник Российского университета дружбы народов. Серия: Юридические науки. 2024. Т. 28. № 3. С. 669-684.

11. Стародубцев И.В., Обласов А.А. Роль блокчейн-эксплорер в криптосистеме // Наука, инновации и технологии: от идей к внедрению. Материалы Всероссийской научно-практической конференции молодых ученых. Комсомольск-на-Амуре, 2025. С. 357-360.

12. Котельвин М.О. Прозрачный блокчейн: тенденции развития государственного контроля за использованием криптовалюты в преступной деятельности // Право и государство: теория и практика. 2022. № 10 (214). С. 138-139.
13. Васюков В.Ф., Старжинская А.Н. Об оперативно-розыскных и следственных мерах противодействия легализации преступных доходов с использованием криптовалют // Российское право: образование, практика, наука. 2024. № 4. С. 68-78.
14. Чихрадзе А.М. Система блокчейн: криминалистический аспект // Философия права. 2024. № 3 (110). С. 187-192.
15. Каторгина Н.П., Тонков Е.Е. Формы использования специальных знаний в российском судопроизводстве // Юридические науки и образование. 2019. № 60. С. 202-220.

REFERENCES

1. Lobachov L.L., Kutsakov F.V. Tsifrovaya kriminalistika: vozmozhnosti i perspektivy razvitiya // Voprosy studencheskoy nauki. 2022. № 12 (76). S. 398-400.
2. Chelysheva O.V. Neprotsessual'nyye formy ispol'zovaniya spetsial'nykh znaniy pri rassledovanii prestupleniy // Mir yuridicheskoy nauki. 2016. № 1-2. S. 70-76.
3. Zaytsev A.A., Sulayeva D.S. Kriptovalyuta kak element kriminalisticheskoy kharakteristiki prestupleniy // Problemy pravovoy i tekhnicheskoy zashchity informatsii. 2021. № 9. S. 309-310.
4. Samoylo V.A. Kharakternyye osobennosti prestupleniy, svyazannykh s ispol'zovaniyem kriptovalyut // Prestupnost' v SNG: problemy preduprezhdeniya i raskrytiya prestupleniy. Sbornik materialov konferentsii. V 3 ch. Voronezh, 2023. CH. 1. S. 337-338.
5. Rastoropov S.V. Tsifrovyye dokazatel'stva v rassledovanii prestupleniy // Probely v rossiyskom zakonodatel'stve. 2020. T. 13. № 5. S. 256-259.
6. Kurin A.A. Sovershenstvovaniye sistemy informatsionnogo obespecheniya raskrytiya i rassledovaniya prestupleniy // Al'manakh-2018. Volgograd, 2018. S. 126-135.
7. Atlam H.F., Ekuri N., Azad M.A., Lallie H.S. Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions // Electronics. 2024. Vol. 13. № 17. Art. 3568.
8. Lantsova A.V., Khasnutdinov R.R. Problematika virtual'nogo sleda v tsifrovoy kriminalistike // International Journal of Humanities and Natural Sciences. 2020. T. 12-3 (51). S. 149-151.
9. Kardanov R.R., Kurin A.A. Analiticheskaya obrabotka kriminalisticheski znachimoy informatsii // Vestnik Vostochno-Sibirskogo instituta MVD Rossii. 2019. № 2 (89). S. 173-177.
10. Garmayev Yu.P., Osipov G.P. Privlecheniye spetsialista dlya issledovaniya kriptovalyut v ugolovnom, grazhdanskom i arbitrazhnom sudoproizvodstvakh // Vestnik Rossiyskogo universiteta druzhby narodov. Seriya: Yuridicheskiye nauki. 2024. T. 28. № 3. S. 669-684.
11. Starodubtsev I.V., Oblasov A.A. Rol' blokcheyn-eksplorer v kriptosisteme // Nauka, innovatsii i tekhnologii: ot idey k vnedreniyu. Materialy Vserossiyskoy nauchno-prakticheskoy konferentsii molodykh uchenykh. Komsomol'sk-na-Amure, 2025. S. 357-360.
12. Kotel'vin M.O. Prozrachnyy blokcheyn: tendentsii razvitiya gosudarstvennogo kontrolya za ispol'zovaniyem kriptovalyuty v prestupnoy deyatel'nosti // Pravo i gosudarstvo: teoriya i praktika. 2022. № 10 (214). S. 138-139.
13. Vasyukov V.F., Starzhinskaya A.N. Ob operativno-rozysknykh i sledstvennykh merakh protivodeystviya legalizatsii prestupnykh dokhodov s ispol'zovaniyem kriptovalyut // Rossiyskoye pravo: obrazovaniye, praktika, nauka. 2024. № 4. S. 68-78.
14. Chikhradze A.M. Sistema blokcheyn: kriminalisticheskiy aspekt // Filosofiya prava. 2024. № 3 (110). S. 187-192.
15. Katorgina N.P., Tonkov Ye.Ye. Formy ispol'zovaniya spetsial'nykh znaniy v rossiyskom sudoproizvodstve // Yuridicheskiye nauki i obrazovaniye. 2019. № 60. S. 202-220.

ССЫЛКА ДЛЯ ЦИТИРОВАНИЯ

Чихрадзе А.М. Блокчейн-аналитика как непроцессуальная форма использования специальных знаний // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2025. № 2 (80). С. 29-35.