

Научная статья

УДК 343.98

DOI 10.33184/vest-law-bsu-2026.29.21

Синицина Татьяна Николаевна

Байкальский государственный университет, Иркутск, Россия,

tanya.sinitsina.14@mail.ru, <https://orcid.org/0009-0000-3820-9043>

КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТЫ

Аннотация. В условиях цифровизации экономики и активного развития распределенных информационных технологий мошенничество с использованием криптовалюты приобретает повышенную общественную опасность, характеризуется высокой латентностью, транснациональностью и сложностью выявления. Цель исследования – определить содержание и структуру криминалистической характеристики мошенничества с использованием криптовалюты, а также выявить криминалистически значимые признаки, имеющие значение для первоначального этапа расследования. Методы: общенаучные методы анализа и синтеза, индукции и дедукции, а также специальные методы криминалистики, включая системно-деятельностный подход, формально-логический анализ, криминалистическое моделирование и обобщение следственной и судебной практики. Результаты: обосновано, что криминалистическая характеристика мошенничества с использованием криптовалюты обладает самостоятельным практическим значением и выступает информационно-ориентирующей категорией. Выделены ее основные элементы, раскрыта специфика цифровой следовой картины, а также показана роль цифровых следов как основного источника доказательственной информации. Сделан вывод о целесообразности использования криминалистической характеристики при выдвижении следственных версий, планировании расследования и выборе тактических приемов.

Ключевые слова: криминалистическая характеристика, мошенничество, криптовалюта, цифровые следы, расследование преступлений

Для цитирования: Синицина Т.Н. Криминалистическая характеристика мошенничества с использованием криптовалюты / Т.Н. Синицина. – DOI 10.33184/vest-law-bsu-2026.29.20 // Вестник Института права Башкирского государственного университета. – 2026. – № 1. – С. 267–281.

Original article

Sinitsina Tatyana Nikolaevna

Baikal State University, Irkutsk, Russia,

tanya.sinitsina.14@mail.ru, <https://orcid.org/0009-0000-3820-9043>

THE FORENSIC CHARACTERISTICS OF CRYPTOCURRENCY FRAUD

Abstract. In the context of the economy digitalization and the information technologies' active development, cryptocurrency fraud poses an increased social danger and is characterized by a high level of latency, a transnational nature, and difficulties in detection. Purpose: to determine the content and structure of the cryptocurrency fraud's forensic characteristics of and to identify forensically significant features relevant to the initial stage of investigation. Methods: general scientific methods of analysis and synthesis, induction and deduction, as well as special forensic methods, including the systems-and-activity approach, formal logical analysis, forensic modeling, and the generalization of investigative and judicial practice. Results: it is substantiated that the forensic characteristics of cryptocurrency fraud have independent practical significance and function as an information-oriented category. Its main elements are highlighted, the specificity of the digital trace pattern is revealed, and the role of digital traces as a primary source of evidential information is also shown. The study concludes that the use of forensic characteristics is advisable when formulating investigative hypotheses, planning investigations, and selecting tactical techniques.

Keywords: forensic characteristics, fraud, cryptocurrency, digital traces, crime investigation

For citation: Sinitsina T.N. The Forensic Characteristics of Cryptocurrency Fraud. *Vestnik Instituta prava Bashkirskogo gosudarstvennogo universiteta = Bulletin of the Institute of Law of the Bashkir State University*, 2026, no. 1, pp. 267–281. (In Russian). DOI 10.33184/vest-law-bsu-2026.29.20

Введение. Криптовалюта как особая форма имущества становится одним из наиболее распространенных инструментов как легальной экономической деятельности, так и преступной. В российском законодательстве термин «криптовалюта» прямо не закреплен, однако в соответствии с п. 1 ст. 1 Федерального закона от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» цифровая валюта определяется как совокупность электронных данных (цифрового кода или обозначения), используемых в качестве средства платежа и (или)

инвестиций, не являющихся денежной единицей Российской Федерации либо иностранного государства и не имеющих обязанного лица¹.

В этих условиях криптовалюта выступает не только средством совершения преступлений, но и самостоятельным предметом преступного посягательства. Наиболее часто она фигурирует в составе корыстных преступлений, прежде всего мошенничества, в том числе совершаемое с использованием информационно-телекоммуникационных технологий (ст. 159, 159.3, 159.6 УК РФ), кража и иные преступления против собственности, связанные с неправомерным завладением цифровыми активами (ст. 158 УК РФ)².

Криминалистическая характеристика как основа для раскрытия природы данного вида преступлений и повышения эффективности расследования.

Разные ученые-криминалисты предлагают собственные подходы к определению криминалистической характеристики преступления. Например, Р.С. Белкин рассматривал ее как систему сведений о типичных способах подготовки, совершения и сокрытия преступлений, закономерно возникающих следах и типичных следственных ситуациях [1, с. 203–210].

И.Ф. Герасимов рассматривает криминалистическую характеристику преступления как систематизированный комплекс сведений о конкретном виде или группе преступлений, сформированный на основе специализированных исследований. Этот комплекс, по его мнению, является существенным элементом методики расследования, определяет содержание методических рекомендаций и в итоге способствует успешному раскрытию, расследованию и предупреждению преступной деятельности [2, с. 333].

В.В. Клочков определяет криминалистическую характеристику преступлений как совокупность сведений о самом преступлении и сопутствующих ему явлениях. Под ней понимается информация, которая отражает устойчивые, типичные и характерные признаки деяния, его свойства и обстоятельства. Эти данные имеют непосредственное криминалистическое значение, поскольку используются для раскрытия и расследования преступлений [3, с. 24].

И.М. Лузгин рассматривает криминалистическую характеристику преступления как информационную модель преступного события, которая по сути выступает его аналогом. В таком качестве она выполняет несколько важных функций: играет эвристическую и познавательную роль, помогая выявлять следы и способствуя раскрытию преступления; выполняет организационно-методическую функцию, позволяя правильно определить направления рассле-

¹ О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон Российской Федерации от 31 июля 2020 № 259 года // Доступ из справ.-правовой системы «КонсультантПлюс».

² Уголовный кодекс Российской Федерации : Федеральный закон Российской Федерации от 13 июня 1996 года № 63-ФЗ : в редакции от 17 декабря 2025 года // Доступ из справ.-правовой системы «КонсультантПлюс».

дования и рационально построить работу по делу; обладает оценочным значением: сопоставляя признаки конкретного деяния с типичными, она помогает дать им правильную криминалистическую оценку [4].

По мнению Н.П. Яблокова, криминалистическая характеристика рассматривается как особая система знаний, отражающая типичные и криминалистически значимые свойства различных видов преступной деятельности. Ее содержание формируется на основе анализа материальных и идеальных следов, возникающих в результате взаимодействия субъекта преступления с окружающей средой, потерпевшим и иными элементами криминальной ситуации. Эти следы фиксируют особенности механизма, способа и условий совершения преступного деяния, а также позволяют выявить важные сведения о личности правонарушителя, которые, хотя и не всегда являются значимыми для юридической квалификации, обладают особой ценностью для раскрытия и расследования преступлений. Типовая криминалистическая характеристика представляет собой научно-обобщенную модель, отражающую закономерные связи между основными элементами преступной деятельности: способом и механизмом совершения преступления, обстановкой его осуществления, типологическими особенностями субъекта и иными структурными компонентами. Данная модель не имеет универсального содержания, поскольку ее структура определяется видовой спецификой преступления, формой вины и особенностями поведения преступника. В различных ситуациях отдельные элементы могут выступать в качестве доминирующих или второстепенных, что обусловлено характером информации, доступной следствию [5, с. 63–67].

О.П. Грибунов и Н.А. Назырова рассматривают криминалистическую характеристику преступления как научную абстракцию, отражающую познанные закономерности совершения преступлений и обобщающую сведения о криминалистически значимых признаках отдельных видов преступной деятельности. По их мнению, криминалистическая характеристика имеет преимущественно вероятностный и описательный характер и выполняет информационно-ориентирующую функцию в системе частных криминалистических методик. Авторы указывают, что данная категория не воспроизводит преступную деятельность как целостный процесс, а фиксирует лишь наиболее устойчивые элементы и связи, выявленные в результате анализа следственной и судебной практики [6].

Развивая системно-деятельностный подход, ученые А.М. Каминский и Ж.А. Русских обращаются к методу криминалистического моделирования как к более эффективному средству познания преступной деятельности. Он основывается на криминалистической модели, которая позволяет реконструировать не только внешние проявления преступления, но и внутреннюю логику деятельности субъекта, включая особенности мышления, принятия решений и адаптации к изменяющимся условиям. В этом контексте криминалистическая характеристика выступает как предварительный, информационно-описательный уровень познания, тогда как криминалистическая модель отра-

жает более глубокий уровень анализа, ориентированный на выявление причинно-следственных связей и механизмов преступного поведения [7].

Данный подход наиболее последовательно представлен в исследованиях Е.И. Фойгель. Автор рассматривает криминалистическую модель как альтернативную и более совершенную категорию, отличающуюся высокой степенью системности, взаимозависимости и взаимообусловленности элементов. Криминалистическая модель преступной деятельности определяется ею как научная абстракция, искусственно воспроизводящая систему поведенческих актов человека по формированию замысла преступления и его реализации в объективной действительности. По мнению ученого, именно криминалистическая модель способна стать полноценной информационной основой для разработки частных криминалистических методик, поскольку она ориентирована не только на описание типичных признаков преступления, но и на объяснение механизма преступной деятельности в целом [8].

Р.С. Белкин в своих работах последовательно и критически осмысливает развитие теоретического аппарата криминалистики, уделяя особое внимание проблеме необоснованного расширения понятийного поля науки. В этой связи он вводит и разрабатывает категорию «криминалистических фантомов», под которыми понимаются умозрительные научные конструкции, не обладающие достаточной теоретической строгостью, эмпирической подтвержденностью и практической применимостью [1, с. 219–222]. Подобные конструкции нередко воспринимаются как научные достижения, однако фактически создают иллюзию познания и подменяют реальное научное исследование декларативными схемами. Особое место в системе «криминалистических фантомов» занимает криминалистическая характеристика преступления. Автор подчеркивает, что сама по себе идея обобщения типичных признаков преступлений не является ошибочной и исторически обусловлена потребностями следственной практики. Однако в процессе развития науки криминалистическая характеристика нередко стала рассматриваться как универсальный и самодостаточный инструмент познания преступной деятельности, что является, по его мнению, методологически неверным. В таких условиях криминалистическая характеристика утрачивает вспомогательный характер и начинает подменять анализ конкретной следственной ситуации, превращаясь в формализованный перечень элементов, механически воспроизводимый в научных работах и учебной литературе.

Р.С. Белкин указывает, что криминалистическая характеристика преступления по своей природе носит вероятностный и статистический характер, поскольку строится на обобщении повторяющихся признаков, выявленных в массиве уголовных дел [1, с. 222–223]. Следовательно, она не способна адекватно отражать индивидуальные особенности конкретного преступного события и динамику преступной деятельности. Это приводит к тому, что следователь ориентируется не на реальные обстоятельства дела, а на «типовую модель», что снижает эффективность расследования и может способствовать принятию ошибочных тактических решений.

В рамках критики криминалистической характеристики он подчеркивает, что научная категория становится «фантомом» не в силу самого факта своего существования, а в результате неправильного методологического использования. Фантомизация проявляется тогда, когда криминалистической характеристике приписываются функции объяснения механизма преступления, прогнозирования поведения субъекта и конструирования тактики расследования, тогда как по своему назначению она способна выполнять лишь ориентирующую и вспомогательную роль [9, с. 216–233].

В.И. Шиканов признает вероятностный и абстрактный характер криминалистической характеристики, однако не поддерживает вывод о ее «фантомности». Он подчеркивает, что криминалистическая характеристика представляет собой научную абстракцию статистического уровня и выполняет строго определенную ориентирующую функцию. В отличие от Р.С. Белкина, ученый считает, что ограниченность криминалистической характеристики не является основанием для отказа от нее как научной категории [10, с. 18–27].

Аналогичной позиции придерживается И.А. Возгрин, который выступает против радикальной критики криминалистической характеристики преступления, указывая, что она является неотъемлемым элементом частных криминалистических методик. По его мнению, криминалистическая характеристика не подменяет анализ конкретного преступления, а создает исходную информационную базу для выдвижения версий и планирования расследования. И.А. Возгрин подчеркивает, что методологические недостатки связаны не с самой категорией, а с ее формальным применением [11, с. 182–191].

По нашему мнению, криминалистическая характеристика сохраняет самостоятельное значение и практическую востребованность, в том числе применительно к расследованию мошенничества с использованием криптовалюты. Мошенничество с использованием криптовалюты характеризуется высокой латентностью, транснациональным характером, использованием цифровых технологий, анонимных платежных инструментов и распределенных информационных систем. В этих условиях следственная деятельность осуществляется в ситуации дефицита исходной информации, отсутствия прямого контакта между преступником и потерпевшим, а также быстрого изменения способов совершения преступлений. Именно поэтому криминалистическая характеристика данного вида преступлений приобретает особое значение как информационно-ориентирующая научная категория, позволяющая систематизировать типичные признаки преступлений и обеспечить эффективный первоначальный этап расследования.

Таким образом, с учетом специфики мошенничества с использованием криптовалюты структурный состав криминалистической характеристики данного вида преступлений, сформированный из наиболее значимых криминалистических признаков, включает в себя следующие взаимосвязанные элементы:

1. особенности личности преступника;
2. способ совершения преступления;
3. особенности личности потерпевшего;

4. обстановку совершения преступления;
5. следовую картину.

Системная взаимосвязь элементов криминалистической характеристики и обусловленность их составляющих. Важное место в криминалистической характеристике занимает личность преступника, как правило, обладающего высокой технической компетентностью, знаниями в области криптографии, блокчейн-технологий и методов сокрытия цифровых следов. Личность потерпевшего также характеризуется определенной типичностью – недостаточным уровнем знаний о кибербезопасности, высокой доверчивостью или неумением анализировать риски цифровых финансовых операций [12, с. 35]. Личность преступника определяет характер способа подготовки, совершения и сокрытия преступления, поскольку интеллектуальные, технические, психологические и мотивационные особенности субъекта непосредственно влияют на выбор применяемых действий и средств.

В то же время сам способ преступления отражает свойства личности правонарушителя, позволяя судить о его компетентности, опыте, уровне подготовки и доступе к специализированным ресурсам. Выбранный преступником способ формирует механизм преступления – последовательность действий, реализуемую в конкретных условиях. Это напрямую определяет тип, структуру и локализацию следов.

Особенности личности потерпевшего также находятся во взаимосвязи со способом преступления: знания, навыки, уровень доверчивости, техническая грамотность или социально-психологические характеристики определяют уязвимость к определенным методам воздействия, прежде всего в случаях мошенничества. Эти свойства нередко становятся частью механизма преступления, влияя на характер взаимодействия между преступником и потерпевшим и на следовые проявления.

Обстановка совершения преступления, включающая как физические, так и цифровые условия, оказывает влияние на выбор преступником тех или иных приемов, на возможности их реализации и на способы скрытного поведения. Она же влияет на форму и объем следов: техническая среда, используемые устройства, программные инструменты или особенности помещений задают параметры их образования и фиксации. Обстановка совершения мошенничества с использованием криптовалюты имеет виртуальный характер и формируется в условиях функционирования распределенных информационных систем, онлайн-платформ и сетевых коммуникаций. Она определяется совокупностью технических средств, программных инструментов и цифровой инфраструктуры, используемых преступником и потерпевшим в процессе взаимодействия. Децентрализованная архитектура блокчейна, отсутствие единого контролирующего центра, трансграничность криптовалютного оборота, возможность применения анонимизирующих сервисов, а также использование интернет-платформ, криптовалютных бирж, мессенджеров и социальных сетей создают специфическую криминальную среду, отличающуюся высокой технологично-

стью и трудностью контроля. В этой среде осуществляется подготовка, реализация и сокрытие преступления, в том числе посредством использования VPN, TOR, прокси-серверов, криптовалютных миксеров и иных инструментов, усложняющих установление участников противоправной деятельности и фиксацию их действий.

Следовая картина является результирующим отражением всех элементов преступной деятельности: она формируется в процессе взаимодействия преступника с обстановкой, объектом посягательства и потерпевшим, отражая способы действий, условия их реализации, технические средства, личностные особенности участников и динамику происходящего.

Следовая картина при данном виде мошенничества формируется преимущественно в цифровой среде и включает данные распределенных реестров, сетевые метаданные, записи логов, информацию, оставляемую на криптовалютных биржах и в сервисах хранения цифровых активов, а также следы использования инструментов анонимизации и конвертации криптовалют [13]. Именно следовая картина приобретает ключевое криминалистическое значение при расследовании мошенничества с использованием криптовалюты, поскольку в условиях отсутствия непосредственного контакта между преступником и потерпевшим, высокой латентности и транснационального характера противоправной деятельности цифровые следы зачастую выступают основным, а нередко и единственным источником доказательственной информации. Указанные обстоятельства обусловили необходимость разработки классификации цифровых следов, направленной на их систематизацию и упорядочение.

В условиях такой цифровой обстановки формируется особый тип следов. Цифровой след – любая криминалистически значимая компьютерная информация, т.е. сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи [14, с. 90]. Это могут быть данные блокчейна, включающие хэши операций, адреса отправителей и получателей, временные метки и структуру движения активов; сведения, оставляемые на криптовалютных биржах и обменных платформах, включающие данные о регистрации аккаунтов, попытках входа, IP-адресах, использовании двухфакторной аутентификации, операциях ввода и вывода средств; сетевые следы, фиксирующие параметры маршрутизации трафика, историю подключений и особенности использования анонимизирующих сервисов; следы взаимодействия в мессенджерах и социальных сетях, такие как переписка, переданные файлы, метаданные сообщений; а также следы использования криптокошельков, включающие данные о создании, импорте и синхронизации кошельков, остатках баланса и связях между адресами. Цифровые следы отражают механизм совершения преступления и обладают значительным криминалистическим потенциалом, поскольку фиксируются в технических устройствах, лог-файлах, распределенных реестрах и серверных системах [15, с. 134].

Особенность цифровых следов состоит в их устойчивости, многоуровневой структуре и распределенности между различными платформами и сетевыми ресурсами. Преступника скрывает свои действия путем усложнения цепочек

транзакций, применения миксеров или анонимизирующих инструментов, цифровые следы сохраняются в результате объективного функционирования блокчейн-технологии и систем логирования.

Следовательно, характеристика становится наиболее значимой и практикоориентированной именно тогда, когда ее элементы наполняются специфическим содержанием, обусловленным природой объекта посягательства, используемыми способами и особенностями криминальной среды. В этой связи обращение к криминалистической характеристике мошенничества с использованием криптовалюты позволяет выявить те особенности, которые отличают данный вид преступной деятельности от традиционных форм мошенничества и обуславливают необходимость применения специализированных методик расследования.

Данные выводы подтверждаются материалами международной судебной практики, в частности уголовным делом в отношении гражданина А.В. Винника, связанным с деятельностью криптовалютной биржи BTC-e. Расследование осуществлялось при координации Интерпола с участием правоохранительных органов Российской Федерации. Анализ материалов данного дела позволяет наглядно проследить проявление основных криминалистически значимых признаков рассматриваемого вида преступлений³.

Способ совершения преступления выражался в использовании криптовалютной биржи в качестве инструмента незаконного оборота и легализации цифровых активов, полученных преступным путем. Преступная деятельность включала прием, конвертацию и перераспределение криптовалюты через подконтрольные адреса, а также применение многоступенчатых транзакций, направленных на сокрытие происхождения средств. Обстановка совершения преступления носила преимущественно виртуальный и транснациональный характер и формировалась в условиях функционирования распределенных информационных систем и международной криптовалютной инфраструктуры, что обусловило необходимость международного взаимодействия, в том числе по линии Интерпола. Личность преступника характеризовалась высоким уровнем технической и финансовой компетентности, знанием принципов работы криптовалютных платформ и способов сокрытия цифровых следов, что напрямую определяло выбор способа совершения преступления. Личность потерпевших, напротив, отличалась ограниченным пониманием механизмов обращения цифровых активов, что способствовало их вовлечению в противоправные схемы. Следовая картина по делу была представлена совокупностью цифровых следов, включая данные блокчейна, сведения о криптовалютных транзакциях, информацию, полученную от криптовалютных бирж, и сетевые логи. Анализ указанных следов позволил установить движение цифровых активов и реконструировать механизм преступной деятельности.

³ Интерпол [Электронный ресурс]. URL: <https://www.interpol.int/> (дата обращения: 12.12.2025).

Необходимо понимать методы фиксации и анализа цифровых следов, оставленных преступниками в сети. Они могут включать IP-адреса, логи серверов, информацию из облачных хранилищ. Работа с такими следами требует учета специфики получения информации с различных технических устройств, а также знания законодательства о защите персональных данных [16, с. 39].

В целях упорядочивания и анализа цифровых следов целесообразно классифицировать их по месту локализации. В зависимости от данного критерия цифровые следы могут быть разделены на:

1. следы, содержащиеся на технических устройствах преступника;
2. следы, зафиксированные на технических устройствах потерпевшего;
3. следы, находящиеся на иных технических устройствах и информационных ресурсах, подключенных к сети Интернет или другим сетям связи (серверы провайдеров, криптовалютных бирж, платежных сервисов, облачных платформ и т. д.).

Расследование преступлений данной категории осуществляется по двум основным направлениям: от общественно опасных последствий к установлению личности преступника и от установленного преступника к совершенным им деяниям.

Наряду с классификацией цифровых следов по месту их локализации представляется целесообразным использовать дополнительные критерии систематизации, позволяющие более полно раскрыть их криминалистическое значение при расследовании мошенничества с использованием криптовалюты.

1. Цифровые следы могут быть классифицированы по характеру отражаемой преступной деятельности:

- следы подготовки;
- следы совершения;
- следы сокрытия преступления.

К следам подготовки относятся сведения о создании криптокошельков, регистрации аккаунтов на криптовалютных биржах, приобретении доменных имен, настройке анонимизирующих сервисов, подготовке фишинговых сайтов или мошеннических платформ. Следы совершения преступления включают данные о криптовалютных транзакциях, переписку с потерпевшими, факты перевода цифровых активов, взаимодействие с криптовалютными биржами и сервисами обмена. Следы сокрытия преступления выражаются в использовании миксеров, анонимизирующих сервисов, многоступенчатых переводов, конвертации цифровых активов, а также в удалении или маскировании цифровых данных.

2. Цифровые следы целесообразно разграничивать по степени их изменчивости:

- устойчивые;
- изменяемые.

К устойчивым относятся следы, зафиксированные в распределенных реестрах (блокчейне), системных логах серверов, инфраструктуре криптовалютных бирж и иных сервисах, где сохранность данных обеспечивается независи-

мо от воли пользователя. Изменяемые цифровые следы включают локальные файлы, временные данные, кэшированные данные, сообщения в мессенджерах и социальных сетях, которые могут быть удалены, искажены или модифицированы преступником.

3. Цифровые следы могут быть классифицированы по уровню их доступности для следствия:

- открытые;
- условно доступные;
- ограниченно доступные.

Открытые цифровые следы представлены публичными данными блокчейна, доступными для анализа без получения специальных разрешений. Условно доступные следы формируются в инфраструктуре криптовалютных бирж, платежных сервисов и онлайн-платформ и могут быть получены по запросам правоохранительных органов. Ограниченно доступные следы связаны с данными, защищенными шифрованием, находящимися в закрытых сетях либо требующими международного правового взаимодействия.

4. Цифровые следы целесообразно классифицировать по их доказательственному значению:

- прямые;
- косвенные.

Прямые цифровые следы непосредственно указывают на факт преступной деятельности. Например, данные о переводе криптовалюты на адрес, контролируемый преступником. Косвенные цифровые следы не подтверждают преступление напрямую, однако позволяют установить связи между участниками, реконструировать механизм преступной деятельности и подтвердить иные доказательства, включая метаданные сетевых подключений и временные корреляции активности.

5. Выделение цифровых следов по уровню их агрегированности:

- элементарные;
- комплексные.

Элементарные цифровые следы представляют собой отдельные события или данные, такие как единичная транзакция, отдельный лог-файл или сообщение. Комплексные цифровые следы формируются в результате анализа совокупности элементарных следов и позволяют выявить схемы мошенничества, цепочки транзакций, роли участников и структуру преступной деятельности в целом.

Взаимосвязь между обстановкой совершения преступления и цифровыми следами является прямой и причинно-обусловленной. Именно характер используемых технических средств, каналы коммуникации, специфика платформ и механизмов перевода активов определяют тип, объем, структуру и локализацию следов.

Заключение. На основании проведенного исследования можно сделать вывод о том, что практическое значение криминалистической характеристики

мошенничества с использованием криптовалюты выражается в возможности ее использования на первоначальном этапе расследования для выдвижения и проверки следственных версий, определения приоритетных направлений поиска доказательственной информации и прогнозирования возможных способов противодействия расследованию. На ее основе осуществляется планирование расследования, включая определение последовательности и содержания первоначальных следственных действий, а также тактических приемов их проведения. Криминалистическая характеристика позволяет обосновать необходимость привлечения специалистов в области информационных технологий, цифровой криминалистики, финансового анализа, блокчейн-аналитики, а также определить объем и характер специальных знаний, требуемых для исследования цифровых следов. Она служит методологической основой для разработки алгоритмов деятельности следователя, ориентированных на выявление, фиксацию, анализ и оценку цифровых следов, установление движения криптовалютных активов и реконструкцию механизма преступной деятельности.

Таким образом, криминалистическая характеристика мошенничества с использованием криптовалюты не подменяет анализ конкретной следственной ситуации, а обеспечивает научно обоснованную информационную базу, способствующую рациональной организации расследования и повышению его результативности.

Список источников

1. Белкин Р.С. Криминалистика: проблемы, тенденции, перспективы. От теории – к практике : монография / Р.С. Белкин. – Москва : Юридическая литература, 1988. – 304 с.
2. Криминалистика : учебник для вузов / А.А. Беляков, И.Ф. Герасимов, А.Н. Гусаков и др. ; под ред. И.Ф. Герасимова, Л.Я. Драпкина. – Москва : Высшая школа, 1994. – 527 с.
3. Криминалистическая характеристика преступлений: состояние и перспективы исследований : сборник научных трудов / отв. ред. Клочков В.В. – Москва : ВИИПиПП, 1984. – 106 с.
4. Лузгин И.М. Некоторые аспекты криминалистической характеристики и место в ней данных о сокрытии преступлений / И.М. Лузгин // Криминалистическая характеристика преступлений : сборник научных трудов. – Москва : Всесоюз. ин-т по изуч. причин и разраб. мер предупреждения преступности, 1984. – С. 27–28.
5. Криминалистика : учебник для студентов вузов, обучающихся по направлению 521400 «Юриспруденция» и специальности 021100 «Юриспруденция» / Т.С. Волчецкая и др. ; отв. ред. Н.П. Яблоков. – 3-е изд., перераб. и доп. – Москва : Юристъ, 2005. – 781 с.

6. Грибунов О.П. Эволюция взглядов на понятие и структуру криминалистической характеристики преступлений / О.П. Грибунов, Н.А. Назырова // Известия ТулГУ. Экономические и юридические науки. – 2020. – № 2. – С. 7–18.
7. Каминский А.М. Некоторые аспекты использования компьютерного сленга для решения задач расследования преступлений в сфере компьютерной информации / А.М. Каминский, Ж.А. Русских // Пермский юридический альманах. – 2019. – № 2. – С. 665–672.
8. Фойгель Е.И. О криминалистической модели человеческой деятельности, связанной с совершением адвентальных преступлений / Е.И. Фойгель // Вестник Казанского юридического института МВД России. – 2018. – Т. 9, № 3. – С. 418–424.
9. Белкин Р.С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики / Р.С. Белкин. – Москва : Норма, 2001. – 237 с.
10. Шиканов В.И. Криминалистическая виктимология и практика расследования убийств : учебное пособие / В.И. Шиканов. – Иркутск : ИГУ, 1979. – 45 с.
11. Возгрин И.А. Введение в криминалистику : история, основы теории, библиография / И.А. Возгрин. – Санкт-Петербург : Юридический центр Пресс, 2003. – 473 с.
12. Рясков А.А. Проблемные аспекты расследования преступлений, совершенных с использованием криптовалюты / А.А. Рясков // Human Progress. – 2024. – Т. 10, Вып. 11. – С. 35–42.
13. Галушин П.В. Специальные технические знания в области цифровой валюты и майнинга, необходимые сотрудникам органов внутренних дел для раскрытия и расследования преступлений, совершаемых с использованием информационно-коммуникационных технологий / П.В. Галушин // Вестник Сибирского юридического института МВД России. – 2024. – № 3 (56). – С. 156–161.
14. Россинская Е.Р. Контрафактный информационно-компьютерный продукт как объект криминалистического исследования компьютерных средств и систем / Е.Р. Россинская, А.И. Семикаленова // Lex Russica. – 2020. – № 8 (165). – С. 86–95.
15. Багмет А. М. Цифровые следы преступлений : монография / А.М. Багмет, В.В. Бычков, С.Ю. Скобелин, Н.Н. Ильин. – Москва : Проспект, 2021. – 168 с.
16. Степаненко Д.А. Цифровая реальность и криминалистика / Д.А. Степаненко // Глаголь правосудия. – 2018. – № 3 (17). – С. 38–43.

References

1. Belkin R.S. Criminalistics: Problems, Trends, Prospects. From Theory to Practice: Monograph. Moscow, Yuridicheskaya Literatura, 1988. 304 p. (In Russian).
2. Gerasimov I.F., Drapkin L.Ya. (eds.). Criminalistics: Textbook for Universities. 2nd ed. Moscow, Vysshaya Shkola, 1994. 528 p. (In Russian).

3. Klochkov V.V. (ed.). *Criminalistic Characteristics of Crimes: State and Prospects of Research: Collection of Scientific Papers*. Moscow, All-Union Institute for the Study and Development of Crime Prevention Measures, 1984. 106 p. (In Russian).
4. Luzgin I.M. Some Aspects of Criminalistic Characteristics and the Place of Data on Concealment of Crimes in It. *Criminalistic Characteristics of Crimes. Collection of Scientific Papers*. Moscow, All-Union Institute for the Study and Development of Crime Prevention Measures, 1984, pp. 27–28. (In Russian).
5. Yablokov N.P. (ed.). *Criminalistics: Textbook. 3rd ed.* Moscow, Yurist, 2005. 781 p. (In Russian).
6. Gribunov O.P., Nazyrova N.A. Evolution of Views on the Concept and Structure of Forensic Characteristics of Crimes. *Izvestiya Tula State University. Economic and Legal Sciences*, 2020, no. 2, pp. 7–18. (In Russian).
7. Kaminsky A.M., Russkikh Zh.A. Some Aspects of Using Computer Slang Words for Solving the Tasks of Investigation Crimes in the Sphere of Computer Information. *Perm Legal Almanac*, 2019, no. 2, pp. 665–672. (In Russian).
8. Foygel E.I. On Criminalistic Model of Human Activity Associated with the Commission of Ethnical Crimes. *Bulletin of the Kazan Law Institute of the MIA of Russia*, 2018, no. 3, pp. 418–424. (In Russian).
9. Belkin R.S. *Criminalistics: Problems of Today. Topical Issues of Russian Criminalistics*. Moscow, Norma, 2001. 237 p. (In Russian).
10. Shikanov V.I. *Forensic Victimology and the Practice of Investigating Murders: Textbook*. Irkutsk, ISU, 1979. 45 p. (In Russian).
11. Vozgrin I.A. *Introduction to Criminalistics: History, Theoretical Foundations, Bibliography*. St. Petersburg, Legal Center Press, 2003. 473 p. (In Russian).
12. Ryasov A.A. Problematic Aspects of the Investigation Crimes Committed Using Cryptocurrency. *Human Progress*, 2024, vol. 10, no. 11, pp. 35–42. (In Russian).
13. Galushin P.V. Special Technical Knowledge in the Field of Digital Currency and Mining, Which Are Necessary for Law Enforcement Officers to Investigate Crimes Committed Using Information and Communication Technologies. *Vestnik of Siberian Law Institute of the MIA of Russia*, 2024, no. 3 (56), pp. 156–161. (In Russian).
14. Rossinskaya E.R., Semikalenova A.I. Counterfeit Information and Computer Product as an Object of Forensic Research of Computer Tools and Systems. *Lex Russica*, 2020, no. 8 (165), pp. 86–95. (In Russian).
15. Bagmet A.M., Bychkov V.V., Skobelin S.Yu., Ilyin N.N. *Digital Traces of Crimes: Monograph*. Moscow, Prospekt, 2021. 168 p. (In Russian).
16. Stepanenko D.A. Digital Reality and Criminalistics. *Glagol'b Pravosudiya*, 2018, no. 3 (17), pp. 38–43. (In Russian).

Информация об авторе**Information about the Author**

Синицина Татьяна Николаевна – Sinitsina Tatyana Nikolaevna – Post-graduate Student

Статья поступила в редакцию 23.12.2025; одобрена после рецензирования 19.01.2026; принята к публикации 30.01.2026.

The article was submitted 23.12.2025; approved after reviewing 19.01.2026; accepted for publication 30.01.2026.