

На правах рукописи



Гайсин Нурсултан Ильгизович

**ПЕРВОНАЧАЛЬНЫЙ ЭТАП РАССЛЕДОВАНИЯ
ДИСТАНЦИОННЫХ ХИЩЕНИЙ КРИПТОВАЛЮТНЫХ АКТИВОВ**

5.1.4. Уголовно-правовые науки

АВТОРЕФЕРАТ

диссертации на соискание ученой степени

кандидата юридических наук

Уфа – 2026

Работа выполнена на кафедре криминалистики Института права федерального государственного бюджетного образовательного учреждения высшего образования «Уфимский университет науки и технологий»

Научный руководитель – **Макаренко Илона Анатольевна,**
доктор юридических наук, профессор

Официальные оппоненты: **Комаров Игорь Михайлович,**
доктор юридических наук, профессор,
заведующий кафедрой криминалистики
юридического факультета ФГБОУ ВО
«Московский государственный
университет имени М.В. Ломоносова»

Русман Галина Сергеевна,
доктор юридических наук, доцент,
заведующий кафедрой уголовного
процесса, криминалистики и судебной
экспертизы ФГАОУ ВО «Южно-
Уральский государственный университет
(национальный исследовательский
университет)»

Ведущая организация Федеральное государственное бюджетное
образовательное учреждение высшего
образования «Кубанский государственный
университет», г. Краснодар

Защита диссертации состоится «02» апреля 2026 г. в 13.00 часов на заседании совета по защите диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук 24.2.479.09, созданного на базе ФГБОУ ВО «Уфимский университет науки и технологий», по адресу: 450005, г. Уфа, ул. Достоевского, д. 131, ауд. 317

С диссертацией можно ознакомиться в библиотеке и на официальном сайте ФГБОУ ВО «Уфимский университет науки и технологий» (<https://uust.ru>)

Автореферат разослан « ___ » _____ 2026 г.

Ученый секретарь
диссертационного совета,
кандидат юридических наук, доцент



Гизатуллин Ирек Альфредович

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Мы живем в эпоху формирования нового технологического уклада, где благодаря развитию информационных технологий на смену старым моделям работы или производства приходят новые. Не менее быстрыми темпами развивается и распространяется использование информационных технологий в преступных целях. Без знания основ, а также особенностей, которые свойственны новейшим информационным технологиям, невозможно сформировать систему знаний о закономерностях и механизмах совершения преступлений в данной сфере, равно как невозможно сформировать систему знаний о тактике и методике производства следственных действий, направленных на раскрытие таких преступлений.

Одним из новшеств является технология блокчейн, которая базируется на идее децентрализации. Благодаря этой технологии пользователи сети Интернет имеют возможность владеть, пользоваться и распоряжаться криптовалютой без вмешательства посредников в виде государственных органов и иных регуляторов (например, банков). Криптовалюта имеет реальную ценность и может быть куплена или продана за национальную валюту по рыночному курсу.

Следует также отметить, что свобода держателей криптовалюты ничем не ограничена и с точки зрения перемещения, поскольку для перевозки активов не требуется никаких материальных носителей, при условии, что держатель криптовалютных активов помнит мнемоническую фразу (набор слов, который является шифром от криптовалютного кошелька) или приватный ключ (набор цифр и латинских букв, с помощью которого можно получить доступ к криптовалютным активам).

Криптовалюта на слуху у многих людей по всему миру, а также признана рядом государств. Так, например, криптовалюта биткоин (BTC) признана

государственной валютой Республики Эль-Сальвадор; США предоставили инвесторам возможность покупки ценных бумаг, удостоверяющих право собственности на BTC и эфириум (ETH), на фондовом рынке, признали BTC в качестве стратегического национального запаса. Следует также отметить, что законодательные органы разных государств предпринимают попытки регуляции майнинга, оборота и других действий с криптовалютой (например, международных расчетов).

Отдельно следует отметить, что широкое распространение получила криптовалюта, являющаяся аналогом национальной валюты. Например, USDT, USDC и EURC (криптовалютные аналоги доллара США и евро). Такой криптовалюте несвойственна высокая волатильность, а потому она наиболее пригодна для расчетов.

Поскольку в настоящее время технология стала массовой, должным образом не урегулирована на законодательном уровне, не подразумевает привязку к личности, а безопасное взаимодействие с ней освоило малое количество пользователей, имеются все благоприятные условия для анонимного совершения преступлений. Участились случаи совершения преступлений различной направленности. Одним из наиболее часто совершаемых является дистанционное хищение криптовалютных активов различными способами.

Хищение в дистанционном формате является наиболее предпочтительным для злоумышленника, поскольку последний имеет возможность не раскрывать свою личность, совершать хищения из любой точки мира, а значит, подвергать себя меньшим рискам с точки зрения уголовного преследования.

Именно дистанционные хищения криптовалютных активов представляют наибольший интерес для исследования ввиду многообразия различных схем по реализации преступного умысла, которые на сегодняшний день мало знакомы правоохрнительным органам.

Не дистанционный формат хищений криптовалюты в большинстве

случаев подразумевает открытое хищение чужого имущества или нападение, с целью хищения чужого имущества, которое может быть расследовано с применением разработанной ранее методики расследования грабежей и разбоев.

В этой связи в криминалистической науке все чаще акцентируется внимание на необходимости глубокого анализа и формирования криминалистической характеристики дистанционных хищений криптовалютных активов, организационных особенностей первоначального этапа расследования таких преступлений, типичных следственных ситуаций и версий, а также тактических рекомендаций для производства отдельных следственных действий, которые необходимо произвести в ходе расследования рассматриваемого вида преступлений.

Сотрудники органов предварительного расследования также не обладают вышеуказанными знаниями либо имеют поверхностные знания, которых может быть недостаточно для расследования таких преступлений. Подавляющее большинство опрошенных респондентов ответили, что либо не обладают знаниями о понятийном аппарате криптовалютной экосистемы, либо им знакомо от одного до трех понятий (88 %), чего недостаточно для раскрытия хищений криптовалюты. Также подавляющее большинство опрошенных респондентов считают, что в настоящее время есть необходимость в комплектовании подразделений органов предварительного расследования кадрами, обладающими знаниями о специфике взаимодействия с криптовалютой, в повышении квалификации действующих сотрудников в части взаимодействия с криптовалютой (92 %), а также в создании подразделений, специализирующихся на расследовании преступлений, которые совершены с использованием криптовалюты (75 %). Все опрошенные придерживаются мнения, что в настоящее время квалифицированных кадров, способных эффективно расследовать хищения криптовалюты (особенно в условиях, когда нет никакой информации о личности подозреваемого или этой информации крайне мало), недостаточно (83 %) либо их нет (17 %)

(приложение 1).

Все вышеуказанное подтверждается незначительным количеством рассмотренных уголовных дел. «За последние годы судами рассмотрено более 20 уголовных дел по преступлениям, связанным с посягательством на принадлежащую гражданам криптовалюту или цифровую валюту. Так, судами города Москвы в 2023–2024 годах рассмотрено 7 таких уголовных дел, судами Московской области – 4 дела», – сообщил судья Верховного Суда РФ Евгений Рудаков в интервью от 19.05.2025¹.

При этом, согласно статистическим данным аналитической компании Chainalysis, в 2024 г. наблюдался значительный рост объемов хищений криптовалютных активов. По сравнению с предыдущим годом общий объем украденных средств увеличился на 21,07 %, достигнув отметки в 2,2 млрд долларов США. Параллельно с этим ростом наблюдалось увеличение количества отдельных инцидентов, связанных с несанкционированным доступом и хищением криптовалюты, которые выросли с 282 случаев, зафиксированных в 2023 г., до 303 случаев в 2024 г. Представленные данные свидетельствуют о существенном росте криминальной активности в сфере криптовалют и, как следствие, о необходимости усиления мер по обеспечению безопасности и защите цифровых активов. При этом за последние годы наблюдается рост объемов денежных средств граждан Российской Федерации, вкладываемых в криптовалюты. По экспертным оценкам, ими открыто более 12 млн криптовалютных кошельков, а объем средств на них составляет порядка 2 трлн рублей. Кроме того, по экспертным данным, Российская Федерация занимает третье место в мире по объему мировых майнинговых мощностей².

¹ Верховный Суд РФ : сайт [Электронный ресурс]. URL: https://www.vsrfr.ru/press_center/mass_media/34394/?ysclid=miifn7хухr208441269 (дата обращения: 10.06.2025).

² Титов А.А. Раскрытие и расследование преступлений, совершаемых в отношении и с использованием криптовалюты (российский и зарубежный опыт) : дис. ... канд. юрид. наук : 5.1.4. Москва, 2025. С. 4.

Именно поэтому имеется необходимость в активном пополнении и систематизации вышеуказанных знаний, формировании модели расследования дистанционных хищений криптовалюты, алгоритма действий при выявлении такого преступления и др.

Степень научной разработанности. Вопросы организации и методики расследования хищений криптовалютных активов частично затрагивались в работах М.М. Виноградовой, Ю.В. Гаврилина, И.С. Бедерова, И.В. Гейкиной, О.П. Грибунова, С.И. Усачева, Е.А. Усачевой, И.А. Ишина, Л.Л. Мельника, В.А. Перова, А.В. Рощупкиной, О.Н. Тисен, А.А. Титова, Д.М. Фарахиева, М.А. Филатовой, А.А. Хайдарова, Е.А. Хариной, А.М. Чихрадзе, Д.И. Шнейдеровой, М.О., Янгаевой и др. Однако в них рассмотрены лишь отдельные аспекты расследования хищений криптовалютных активов, комплексного же рассмотрения криминалистической характеристики и криминалистических особенностей первоначального этапа расследования таких преступлений не проводилось.

Объект исследования – криминальная деятельность лиц, совершающих дистанционное хищение криптовалютных активов, а также деятельность органов предварительного расследования и оперативно-розыскных органов по выявлению и расследованию преступлений этого вида.

Предметом диссертационного исследования являются закономерности преступной деятельности по подготовке, совершению и сокрытию дистанционных хищений криптовалютных активов, а также закономерности выявления, раскрытия и первоначального этапа расследования преступлений данного вида.

Цель диссертационного исследования заключается в получении нового знания в криминалистической науке, направленного на совершенствование методики первоначального этапа расследования дистанционных хищений криптовалютных активов, а также в разработке предложений и рекомендаций, позволяющих повысить эффективность расследования этих преступлений.

Для достижения поставленной цели потребовалось решение следующих **задач**:

- рассмотреть понятийный аппарат криптовалютной экосистемы и особенности взаимодействия с технологией блокчейн и криптовалютой, которые сотрудникам правоохранительных органов необходимо знать и применять на практике при расследовании хищений криптовалютных активов;
- выявить часто применяемые преступниками способы дистанционного хищения криптовалютных активов;
- рассмотреть криптовалюту в качестве предмета хищения;
- описать характеристику таких элементов криминалистической характеристики хищения криптовалюты, как цифровые следы, личность преступника, а также личность потерпевшего;
- раскрыть содержание и организационные особенности первоначального этапа расследования дистанционных хищений криптовалютных активов;
- классифицировать систему следственных ситуаций и версий;
- раскрыть особенности взаимодействия органов предварительного расследования с органами, осуществляющими оперативно-розыскную деятельность;
- выявить особенности производства осмотров;
- обобщить особенности производства допроса потерпевшего от хищения криптовалютных активов;
- раскрыть организационные и тактические особенности производства обыска;
- сформулировать организационные особенности назначения и производства экспертиз при расследовании дистанционных хищений криптовалюты.

Методологическая основа исследования представлена общими и частными научными методами познания. В качестве общих методов

выступают: диалектический, системный, функциональный, анализа, синтеза, индукции и дедукции. В числе частных научных методов использовались такие методы, как сравнительно-правовой, историко-правовой, формально-юридический, формально-логический, метод теоретико-правового моделирования, юридико-технический, статистический, конкретно-социологический (анкетирования) и др. Раскрывающим единство объекта в условиях его взаимосвязи с другими явлениями объективной действительности являлся диалектический метод познания. Метод теоретико-правового моделирования применялся при разработке авторской теоретической концепции модели расследования дистанционных хищений криптовалютных активов. Системный подход позволил выявить взаимосвязи между структурными элементами изучаемого объекта. Функциональный метод и синтез позволили выявить и обосновать наличие личностных особенностей преступников, совершающих дистанционное хищение криптовалютных активов. При создании понятийного аппарата, необходимого для разработки настоящей концепции, использовались формально-юридический и формально-логический методы. Практически на всех этапах исследования для обеспечения достоверности выводов и предложений использовались следующие методы: анализ, синтез, индукция, дедукция. Статистический метод обеспечил возможность обобщения результатов изучения практики расследования хищений криптовалютных активов. Социологические методы использовались для выявления мнений и позиций участников уголовного судопроизводства по актуальным для исследования вопросам и для их отношения к отдельным выводам автора.

Теоретическую основу исследования составили труды отечественных ученых в области криминалистики, судебно-экспертной деятельности: В.А. Авериной, Т.В. Аверьяновой, Ф.Г. Аминова, О.Я. Баева, Е.В. Безручко, Р.С. Белкина, Л.В. Бертовского, А.В. Варданяна, Т.С. Волчецкой, Л.Я. Драпкина, Р.И. Зайнуллина, И.М. Комарова, Е.Р. Россинской, А.В. Руденко, Г.С. Русман, Н.А. Подольного, Н.П. Майлис, И.А. Макаренко,

А.Н. Халикова, А.А. Эксархопуло, Н.П. Яблокова и др.

Нормативно-правовую базу диссертационного исследования составили положения УК РФ, УПК РФ, НК РФ, федеральных законов «Об оперативно-розыскной деятельности», «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», постановлений Пленума Верховного Суда РФ от 27 декабря 2002 г. № 20 «О судебной практике по делам о краже, грабеже и разбое», «О судебной практике по делам о мошенничестве, присвоении и растрате», анализ и использование которых обусловлены предметом и задачами исследования.

Эмпирическая база исследования. При подготовке диссертационной работы были изучены материалы 22 уголовных дел о хищении криптовалюты. По специально разработанной анкете проведен опрос 175 сотрудников органов предварительного расследования и судей, также использовались материалы изученной практики другими учеными.

Научная новизна диссертационного исследования заключается в том, что на монографическом уровне комплексно исследованы криминалистические основы, проблемы и особенности первоначального этапа расследования дистанционных хищений криптовалютных активов. Предложена структура криминалистической характеристики дистанционных хищений криптовалютных активов, описаны основные ее элементы, выявлены корреляционные связи между ними. На основе ситуационного подхода выявлены и проанализированы следственные ситуации, складывающиеся на первоначальном этапе расследования, разработаны алгоритмы действий следователя (дознавателя) для их разрешения. Определены особенности и разработаны рекомендации по реализации первичной информации о дистанционном хищении криптовалютных активов. Раскрыто содержание первоначального этапа расследования рассматриваемой категории уголовных дел. Разработаны тактические рекомендации по производству следственных действий и использованию специальных знаний при расследовании

дистанционных хищений криптовалютных активов.

На защиту выносятся следующие положения:

1. Обобщенный комплекс понятийного аппарата криптовалютной экосистемы, а также особенности взаимодействия с технологией блокчейн и криптовалютой, рекомендуемые к изучению и применению при расследовании хищений криптовалюты.

2. Способы хищения криптовалюты чаще всего выражаются:

а) в использовании злоумышленником входных данных (мнемонической фразы, приватного ключа, логина и пароля), позволяющих получить доступ к криптовалютному кошельку (биржевому аккаунту);

б) в предоставлении собственником криптовалюты разрешения вредоносному децентрализованному приложению распоряжаться криптовалютой, в результате чего у злоумышленника появляется возможность распорядиться криптовалютой по своему усмотрению, без доступа к кошельку;

в) в переводе криптовалюты потерпевшим в адрес злоумышленника.

3. Характеристика элементов криминалистической характеристики дистанционного хищения криптовалюты, корреляционные связи между которыми (способ совершения хищения, способ сокрытия следов хищения, цифровые следы, личность потерпевшего) позволяют сделать вероятностный вывод о личности преступника.

4. Обязательные и дополнительные данные, указывающие на признаки преступления, достаточные для возбуждения уголовного дела по факту дистанционного хищения криптовалюты. Обязательные данные, указывающие на признаки преступления, должны иметься в любом материале проверки сообщения о совершенном хищении криптовалюты, а наличие дополнительных данных определяется исходя из возможности точно установить сумму похищенного для возбуждения уголовного дела, способа хранения криптовалюты, а также в зависимости от совершения транзакции – заявителем или злоумышленником.

5. Алгоритм действий следователя (дознавателя), направленный сначала на установление наличия транзакции в блокчейн-обозревателе, взаимодействий кошелька злоумышленника с кошельками криптовалютных бирж и (или) обменников, а далее – на установление лиц, на чье имя зарегистрирован биржевой аккаунт или открыт банковский счет, на который поступили денежные средства в обмен на похищенную криптовалюту, а также лиц, фактически использовавших вышеуказанный биржевой аккаунт или банковскую карту. Обозначены организационные и тактические особенности производства некоторых действий в зависимости от способа хранения криптовалюты, от того, совершена транзакция заявителем или злоумышленником, а также от других обстоятельств и фактов, производных от первых двух.

6. Классификация следственных версий:

1) в зависимости от способа хранения криптовалюты и инициатора транзакции:

если похищенная криптовалюта хранилась на кастодиальном кошельке (биржевом аккаунте) и при этом неправомерную транзакцию совершил злоумышленник:

- хищение криптовалюты совершено в результате получения третьими лицами доступа к биржевому аккаунту заявителя (потерпевшего);
- хищение криптовалюты совершено в результате хакерской атаки на биржу;

если похищенная криптовалюта хранилась на кастодиальном кошельке (биржевом аккаунте) и при этом транзакцию совершил потерпевший:

- хищение криптовалюты совершено в результате обмана или злоупотребления доверием;
- факт хищения отсутствует ввиду добросовестного заблуждения заявителя;

если похищенная криптовалюта хранилась на некастодиальном кошельке и транзакцию по переводу криптовалюты совершил

злоумышленник:

– хищение криптовалюты совершено в результате получения третьими лицами доступа к некастодиальному кошельку заявителя (потерпевшего);

– хищение криптовалюты совершено в результате предоставления разрешения вредоносному децентрализованному приложению распоряжаться криптовалютой;

– хищение криптовалюты совершено в результате хакерской атаки на децентрализованное приложение, если потерпевший разместил свою криптовалюту в этом приложении;

если похищенная криптовалюта хранилась на некастодиальном кошельке и потерпевший сам произвел перевод криптовалюты:

– хищение криптовалюты совершено в результате обмана или злоупотребления доверием;

– факт хищения отсутствует ввиду добросовестного заблуждения заявителя;

2) по признаку связи с потерпевшим:

– хищение совершено посторонним лицом;

– хищение совершено знакомым потерпевшему лицом или по его наводке.

Версию о добросовестном заблуждении лица относительно совершения хищения следует выдвинуть, если транзакция отсутствует или совершена пользователем с ошибками при указании публичного адреса получателя; отсутствуют доказательства, что криптовалюта выбыла из владения пользователя под воздействием обмана, злоупотребления доверием, а также в результате действий третьих лиц.

7. Система оперативно-розыскных мероприятий, в рамках которых необходимо получить информацию о персональных данных лиц, совершивших хищение, а также некоторые вспомогательные инструменты для эффективной реализации оперативно-розыскных задач.

8. Алгоритм действий следователя по установлению наличия транзакций:

- получение объяснения от заявителя (допрос потерпевшего);
- осмотр электронного носителя информации, с которого у заявителя (потерпевшего) имелся доступ к криптовалюте, а именно истории транзакций на криптовалютном кошельке;
- поиск транзакции, в результате совершения которой произошло хищение, в блокчейн-обозревателе через ID транзакции или публичные адреса заявителя (потерпевшего) или злоумышленника (в отсутствие информации об ID транзакции);
- осмотр места происшествия, в котором имеется доступ к электронным носителям информации (если в ходе получения объяснения или допроса нет возможности незамедлительно произвести осмотр электронного носителя информации, с которого имеется доступ к криптовалюте).

9. Организационно-тактические особенности допроса потерпевшего:

- если потерпевший способен самостоятельно пояснить обстоятельства хищения, следует предоставить ему возможность дать показания в форме свободного рассказа, а затем задать уточняющие вопросы;
- следует попросить потерпевшего продемонстрировать доказательства совершения транзакций из блокчейн-обозревателей и истории транзакций в кошельке, переписку с предположительными злоумышленниками и другие доказательства, достоверно подтверждающие его слова;
- необходимо задать вопросы о способе хранения потерпевшим криптовалюта, а также о лице, которое совершало транзакции с криптовалютного кошелька потерпевшего;
- остальные вопросы должны быть заданы исходя из ответов на вышеуказанные вопросы;

– в любом случае необходимо фиксировать все возможные идентификаторы (публичные адреса, ID транзакций, контракты монет и токенов и т. д.).

10. Комплекс тактических приемов, который необходимо применять в ходе обыска:

– необходимо предусмотреть возможность ограничения доступа как к сотовой связи, так и к интернет-связи перед началом проведения обыска, чтобы у обыскиваемых лиц не было возможности просигнализировать сообщникам о необходимости перевести криптовалюту на адрес другого кошелька, а также перемесить или уничтожить информацию, имеющую значение для дела;

– при изъятии электронных носителей информации следует учитывать, что практически все устройства имеют возможность удаленного доступа, поэтому для недопущения дистанционного удаления данных необходимо предпринять действия по ограничению доступа к Сети с изымаемого устройства;

– обращать внимание не только на привычные электронные носители информации, но и на наличие холодных криптовалютных кошельков, а также иные объекты материального мира;

– необходима подготовка к наложению ареста на обнаруженную криптовалюту до ее перевода сообщниками подозреваемого на другой публичный адрес, которая заключается в получении судебного разрешения на наложение ареста на криптовалюту, а также в подготовке криптовалютного кошелька, на адрес которого будет переведена арестованная криптовалюта.

11. Комплекс задач, который необходимо решить в ходе компьютерно-технической и экономической экспертиз:

– восстановление удаленной информации;

– изъятие информации с электронных носителей, принадлежащих подозреваемому;

- восстановление доступа к электронному носителю информации и информации, содержащейся на нем;
- установление рублевой стоимости похищенной криптовалюты.

12. Методика определения стоимости похищенной криптовалюты, особенности которой заключаются в учете наименьшей рыночной стоимости в силу законодательных положений о презумпции невиновности, а также в учете расходов на комиссии, когда незаконную транзакцию совершает злоумышленник.

Теоретическая и практическая значимость исследования обусловлена научным обоснованием разработанных основных положений методического обеспечения расследования дистанционных хищений криптовалютных активов. Сформулированные в нем концептуальные выводы и предложения обогащают теоретическую основу такого раздела науки криминалистики, как методика расследования отдельных видов преступлений.

Результаты диссертационного исследования могут быть использованы в учебном процессе при преподавании криминалистики и иных специальных учебных дисциплин в рамках изучения методики расследования отдельных видов преступлений.

Проведенное исследование позволяет определить пути повышения эффективности борьбы с такими преступлениями, как дистанционное хищение криптовалютных активов, так как содержит теоретические и организационно-методические основы их выявления, раскрытия и расследования.

Результаты диссертации могут быть использованы в практической деятельности следственных и оперативно-розыскных органов по раскрытию и расследованию дистанционных хищений криптовалютных активов.

Апробация и внедрение результатов исследования.

Ход и результаты диссертационного исследования отражены в семи научных работах, четыре из которых опубликованы в рецензируемых научных журналах, рекомендованных Высшей аттестационной комиссией при

Министерстве науки и высшего образования РФ.

Результаты диссертационного исследования докладывались на международных научно-практических конференциях: «Отечественная криминалистика: вчера, сегодня, завтра», посвященной 75-летию кафедры криминалистики Московского государственного университета (Москва, 2025), «Актуальные проблемы использования специальных знаний в уголовном, гражданском, арбитражном процессе и по делам об административных правонарушениях» (Уфа, 2025), «Государство и правоприменение: задачи познания и стимулы развития в условиях цифровизации» (Ростов-на-Дону, 2024).

Структура диссертационного исследования обусловлена его тематикой, целью и задачами. Работа состоит из введения, трех глав, включающих 11 параграфов, заключения, списка литературы и приложений.

ОСНОВНОЕ СОДЕРЖАНИЕ

Во **введении** обосновывается актуальность темы диссертационного исследования, определяются его объект, предмет, цель и задачи, характеризуются методологическая основа, нормативная база и научная новизна работы, формулируются основные положения, выносимые на защиту, освещаются используемый эмпирический материал, теоретическая и практическая значимость, приводятся сведения об апробации полученных результатов.

Первая глава **«Понятийный аппарат криптовалютной экосистемы и криминалистическая характеристика дистанционных хищений криптовалютных активов»** состоит из четырех параграфов.

В первом параграфе *«Понятие криптовалютной экосистемы и ее понятийный аппарат. Его значение для расследования преступлений»* рассматриваются основные понятия криптовалютной экосистемы, знание

которых необходимо для расследования преступлений.

Соискатель раскрывает понятие блокчейна, как основополагающей технологии, без которой невозможно существование криптовалюты, кратко описывает механизмы его работы и свойства, а также указывает на возможность отслеживания транзакций в нем через общедоступные онлайн источники, что является важной частью первоначального этапа предварительного расследования.

Далее подробно рассматриваются понятие, свойства и виды криптовалютного кошелька. Соискатель указывает, что при хранении криптовалюты на кошельке централизованной биржи существует возможность направления запроса в ее адрес и получения сведений о личности, на чье имя был зарегистрирован биржевой аккаунт.

Рассмотрены такие понятия, как публичный и приватный ключ, мнемоническая фраза. Соискатель указывает на то, что большинство хищений совершается благодаря получению доступа к приватным ключам и мнемоническим фразам пользователей.

Раскрыты понятие, свойства и виды криптовалюты. Разграничены такие понятия, как монета, токен и NFT для лучшего понимания предмета хищения.

Даны определения смарт-контракта и децентрализованного приложения. Указано на то, что злоумышленники активно пользуются возможностью анонимно создавать децентрализованные приложения, которые предназначены для совершения хищений криптовалютных активов через функцию предоставления согласия на распоряжение криптовалютой.

Во втором параграфе ***«Понятие криминалистической характеристики дистанционных хищений криптовалютных активов. Криптовалютные активы как предмет преступного посягательства»*** дано определение криминалистической характеристики хищений криптовалютных активов.

Криптовалютные активы рассмотрены в качестве предмета преступного посягательства. Соискатель пришел к выводу, что криптовалютные активы

являются предметом преступного посягательства ввиду законодательного закрепления имущественного статуса за цифровой валютой.

В подтверждение того, что под цифровой валютой подразумевается криптовалюта приведен ряд аргументов, основывающихся на содержании пояснительных записок к законопроектам о придании имущественного статуса цифровой валюте, а также судебной практике вышестоящих судов о хищении криптовалюты.

В третьем параграфе *«Характеристика способов дистанционного хищения криптовалютных активов, как системообразующий элемент криминалистической характеристики»* соискатель указывает на важность анализа возможных способов совершения хищений криптовалюты. Обладая знаниями о способах совершения хищений криптовалютных активов и их технических особенностях, следователи (дознаватели) будут производить допросы, осмотры и другие следственные действия наиболее эффективно, смогут выдвигать типичные следственные версии относительно способа совершения хищения, а также круга лиц, которые могли совершить данное преступление, и исходя из выдвинутых версий, оценивать благоприятность следственной ситуации, планировать дальнейшие действия.

Рассмотрены основные способы совершения хищений криптовалюты:

- 1) в результате использования злоумышленником входных данных (мнемонической фразы, приватного ключа, логина и пароля), позволяющих получить доступ к криптовалютному кошельку (биржевому аккаунту),
- 2) в результате предоставления разрешения вредоносному децентрализованному приложению распоряжаться криптовалютой;
- 3) в результате перевода криптовалюты самим потерпевшим в адрес злоумышленника.

Раскрыты некоторые схемы реализации вышеуказанных способов, среди которых фишинг, использование вредоносных программных обеспечений, а также продажа токенов, не имеющих реальной ценности.

В четвертом параграфе *«Иные элементы криминалистической*

характеристики хищения криптовалютных активов» раскрыты такие элементы криминалистической характеристики хищения криптовалютных активов, как электронные (цифровые) следы, личность преступника и личность потерпевшего.

Раскрывая электронные (цифровые) следы как элемент криминалистической характеристики, указано на конкретные следы, оставляемые при совершении преступления: информация о совершенных транзакциях, файлы (фотографии, видеозаписи, аудиозаписи и т.д.), программные обеспечения, переписки в социальных сетях и мессенджерах, история посещений интернет-ресурсов в браузерах, информация об аккаунтах в социальных сетях и мессенджерах, статистические данные о посещениях интернет-ресурсов, открытии файлов и программных обеспечений, история поисковых запросов, данные о местонахождении и передвижении устройства, его IP-адрес и др. Также указано их значение при расследовании дистанционных хищений криптовалютных активов.

Рассматривая личность преступника, соискатель указал на его молодой возраст в силу недавнего возникновения и развития криптовалютной сферы, а также возможные уровни профессиональной подготовки.

Характеризуя личность потерпевшего, соискатель также аргументированно указал на возможный возраст большинства потерпевших, отсутствие образования в сфере информационных технологий, глубоких знаний в криптовалютной сфере, а также базовых знаний о финансовой грамотности, что делает их более уязвимыми перед злоумышленниками. Описано типичное поведение при взаимодействии как с сетью Интернет, в целом, так и с криптовалютой, в частности, охарактеризованы некоторые личностные качества.

Вторая глава **«Организационные особенности первоначального этапа расследования дистанционных хищений криптовалютных активов»** включает в себя три параграфа.

В первом параграфе **«Основания возбуждения уголовного дела о**

хищении криптовалютных активов, содержание этой стадии расследования» раскрыта основная проблема на стадии возбуждения уголовного дела о хищении криптовалютных активов, которая заключается в определении достаточности оснований для принятия решения о возбуждении уголовного дела.

Соискатель описал алгоритм действий для принятия решения о возбуждении уголовного дела, который состоит в получении объяснения от заявителя, осмотре электронных носителей информации через которые имеется доступ к криптовалюте, а также через которые осуществлялись банковские транзакции, переписки с криптовалютными обменниками, электронные письма от этих обменников о выполненной заявке на покупку криптовалюты, сведения и переписки из peer-to-peer платформ криптовалютных бирж.

Перечислены обязательные и дополнительные основания для возбуждения уголовного дела.

Во втором параграфе *«Типичные следственные ситуации и версии при расследовании хищений криптовалютных активов»* перечислены возможные варианты следственных ситуаций, большинство которых является неблагоприятными в силу дистанционного характера совершенного преступления.

Ввиду открытости сведений об объективных признаках преступления соискатель предлагает для выдвижения перечень типичных следственных версий исходя из способов совершения преступления, указанных в параграфе 1.3.

Далее соискателем предложен ряд версий для выдвижения исходя из способа хранения криптовалюты и инициатора транзакции.

В третьем параграфе *«Взаимодействие следователя с органами, осуществляющими оперативно-розыскную деятельность»* соискателем указано на необходимость взаимодействия следователя (дознателя) с

оперативно-розыскными органами как для оказания помощи в производстве отдельных следственных действий, так и для установления личности подозреваемого.

Формируя поручения для оперативно-розыскных органов, следует указывать на необходимость в ходе оперативно-розыскных мероприятий (наведение справок, опрос, исследование документов) установить:

1. Принадлежит ли криптовалютный кошелек, в адрес которого поступили средства в результате хищения, какой-либо криптовалютной бирже или обменнику, а также места их регистрации и нахождения;

2. Принадлежат ли криптовалютные кошельки, связанные транзакциями с вышеуказанным кошельком, криптовалютной бирже или обменнику, а также места их регистрации и нахождения;

3. Имеются ли упоминания о вышеуказанных кошельках в сети Интернет, в том числе в социальных сетях и мессенджерах.

Если в ходе оперативно-розыскных мероприятий удалось установить принадлежность какого-либо из кошельков бирже, необходимо получить информацию о лице, на чье имя зарегистрирован биржевой аккаунт, информацию об IP-адресах, выданных электронным носителям информации, использованным для совершения преступлений, провайдерах, обслуживавших данные IP-адреса, а также адреса проживания и данные о личностях, выступавших сторонами по договорам оказания услуг по предоставлению доступа в Интернет.

Указан различный инструментарий, который может быть использован для установления личности подозреваемого.

Третья глава **«Тактические особенности производства отдельных следственных действий на первоначальном этапе расследования дистанционных хищений криптовалютных активов»** состоит из четырех параграфов.

В первом параграфе **«Особенности производства следственного осмотра»** указано на основные объекты осмотра, которыми являются

блокчейн-обозреватели и криптовалютные кошельки, и данные, которые необходимы для осмотра этих объектов, поскольку их осмотр – единственный способ, позволяющий объективно установить и проверить наличие той или иной транзакции, время ее совершения, количество и наименование криптовалюты, с которой была совершена операция, адреса кошельков, в пользу которого был совершен перевод, а также адреса кошельков, с которых поступили средства на осматриваемый кошелек, балансы кошельков, чьи транзакции стали предметом осмотра, и другую информацию.

При наличии возможности, осмотр следует произвести сразу после допроса (получения объяснения). Если же у потерпевшего (заявителя) нет при себе электронного носителя информации, откуда имеется доступ к криптовалюте, или при нем не все электронные носители информации, откуда имеется доступ к криптовалюте, необходимо произвести осмотр указанных объектов по месту жительства потерпевшего (заявителя). Это позволит не упустить важную информацию в ходе расследования.

Перед проведением осмотра целесообразно наладить взаимодействие со специалистами для получения консультативной помощи и помощи во время непосредственного осмотра.

Приведены примеры того, как выглядят транзакции в блокчейн-обозревателе. Описаны особенности осмотра криптовалютного кошелька.

Для полного и всестороннего расследования указано, что осмотрам должны быть подвергнуты и другие объекты: истории посещения браузеров (особое внимание следует обратить на историю посещения браузера, встроенного в кошелек, если он был установлен на смартфон), конкретные страницы в сети Интернет (в том числе и децентрализованные приложения), страницы социальных сетей, мессенджеры, электронные почты и другие сервисы, в которых имеется возможность вести переписки. Также следует исходить из ранее полученных объяснений от потерпевшего и результатов осмотра блокчейн-обозревателя и криптовалютного кошелька.

Во втором параграфе *«Особенности допроса потерпевшего от хищения криптовалюты»* указано на необходимость взаимодействия со специалистами для получения консультативной помощи при подготовке к допросу, раскрыта тактика проведения допроса потерпевшего, а также перечень обстоятельств, которые необходимо установить первоочередно для планирования и проведения других следственных действий, выдвижения следственных версий и принятия последующих мер.

При этом показания потерпевшего необходимо проверять в ходе других следственных действий, поскольку допрашиваемый может как добросовестно заблуждаться относительно своих показаний, по разным причинам не упомянуть о важных событиях и фактах, либо намеренно вводить следователя в заблуждение.

В третьем параграфе *«Тактические особенности организации и производства обыска»* указаны объекты обыска, предметы, которые могут быть изъяты в ходе этого следственного действия.

В ходе проведения обыска необходимо обращать внимание не только на привычные для нас электронные носители информации, под которыми мы подразумеваем персональные компьютеры, ноутбуки, планшеты, смартфоны, флеш-накопители и прочие привычные для современного человека носители информации, но также и на те объекты, которые внешне не напоминают электронные носители информации и криптовалютные кошельки, но могут ими являться.

В качестве организационных и тактических особенностей указано на необходимость подготовки к наложению ареста на криптовалюту, привлечение к участию лица, обладающего знаниями в сфере информационных технологий и имеющего практический опыт работы с криптовалютными сервисами, а также ограничение доступа к связи и ликвидации доступа к сети на изымаемых устройствах.

Для наложения ареста на криптовалюту необходимо поручить проведение обыска дознавателю или органу дознания для того, чтобы

следователь параллельно обыску имел возможность наложить арест на обнаруженную криптовалюту.

В четвертом параграфе «Тактика назначения и производства судебных экспертиз при расследовании хищений криптовалюты» рассмотрены компьютерно-техническая и экономическая экспертизы. Указаны объекты, в отношении которых должна быть проведена компьютерно-техническая экспертиза, обоснована необходимость проведения экономической экспертизы, а также приведен примерный перечень вопросов, которые необходимо поставить перед лицами, обладающими специальными знаниями.

При невозможности определить вредоносность децентрализованного приложения экспертным путем ввиду закрытого исходного кода децентрализованного приложения, предложено проводить следственный эксперимент, направленный на проверку возможности совершения действий, при которых могли быть похищены криптовалютные активы.

В заключении подведены итоги исследования, представлены научно обоснованные выводы и предложения, кратко изложены научно-практические рекомендации по организации и проведению расследования дистанционных хищений криптовалютных активов.

В приложении представлены результаты проведенного опроса сотрудников правоохранительных органов и судей, а также примеры того, как выглядят различные транзакции в блокчейн-обозревателе.

ОСНОВНЫЕ НАУЧНЫЕ РЕЗУЛЬТАТЫ ДИССЕРТАЦИИ ОПУБЛИКОВАНЫ В СЛЕДУЮЩИХ РАБОТАХ АВТОРА:

Научные статьи, опубликованные в рецензируемых научных журналах и изданиях, рекомендованных Высшей аттестационной комиссией при Министерстве науки и высшего образования РФ:

1. К вопросу о необходимости криминалистического обеспечения

расследования хищений криптовалютных активов // Вестник Института права Башкирского государственного университета. – 2024. – № 4(24). – С. 154-160.

2. К вопросу об элементах криминалистической характеристики хищения криптовалютных активов // Философия права. – 2025. – № 2. – С. 113-118.

3. Характеристика способов совершения хищений криптовалютных активов // Сибирские уголовно-процессуальные и криминалистические чтения. – 2025. – № 3. – С. 30-39.

4. К вопросу о некоторых организационных и тактических особенностях производства допроса потерпевшего по делам о хищении криптовалютных активов в форме кражи и мошенничества // Вестник Института права Башкирского государственного университета. – 2025. – № 4(28). – С. 285-298.

Научные статьи, опубликованные в иных научных изданиях:

5. Проблемы определения стоимости похищенной криптовалюты по делам о хищении криптовалютных активов // Государство и правоприменение: задачи познания и стимулы развития в условиях цифровизации: материалы международной научно-практической конференции. – Ростов-на-Дону, 2024. – С. 3-10.

6. К вопросу о некоторых организационных и тактических особенностях производства осмотра криптовалютных кошельков и блокчейн-обозревателей по делам о хищении криптовалютных активов // Актуальные проблемы использования специальных знаний в уголовном, гражданском, арбитражном процессе и по делам об административных правонарушениях: материалы XIV научно-практической конференции. – Уфа, 2025. – С. 46-53.

7. К вопросу о проверке обстоятельств и фактов, позволяющих выдвинуть типичные следственные версии хищения криптовалютных активов // Отечественная криминалистика: вчера, сегодня, завтра: материалы научно-практической конференции, посвященной 75-летию со дня образования кафедры криминалистики Юридического факультета МГУ. – Москва, 2025. – С. 224-229.