МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»

На правах рукописи

Гайсин Нурсултан Ильгизович

ПЕРВОНАЧАЛЬНЫЙ ЭТАП РАССЛЕДОВАНИЯ ДИСТАНЦИОННЫХ ХИЩЕНИЙ КРИПТОВАЛЮТНЫХ АКТИВОВ

Специальность 5.1.4. Уголовно-правовые науки
(юридические науки)

ДИССЕРТАЦИЯ
на соискание ученой степени
кандидата юридических наук

Научный руководитель
доктор юридических наук,
профессор
Макаренко Илона Анатольевна

Уфа – 2026

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

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 биткойн (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 диссертационного исследования ввиду многообразия различных схем по реализации преступного умысла, которые на сегодняшний день мало знакомы правоохранительным 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 19.05.2025[1].

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 мощностей[2].

Именно поэтому имеется необходимость в активном пополнении и

---

[1] Верховный Суд РФ : сайт [Электронный ресурс]. URL: https://www.vsrf.ru/press_center/mass_media/34394/?ysclid=miifn7xyxr208441269 (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.

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. Аминева, 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 дистанционного 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.

Глава 1. Понятийный аппарат криптовалютной экосистемы и криминалистическая характеристика дистанционных хищений криптовалютных активов

1.1. Понятие криптовалютной экосистемы и ее понятийный аппарат. Его значение для расследования преступлений

Для эффективной организации первоначального этапа расследования, выдвижения следственных версий, а также результативного проведения отдельных следственных действий и правильной фиксации их результатов по уголовным делам о хищении криптовалютных активов, необходимо обладать знаниями о технологии, благодаря которой появилась и функционирует любая криптовалюта, об инструментах, используемых для взаимодействия с криптовалютой, а также об особенностях взаимодействия с криптовалютой. Большинство опрошенных респондентов (95%) в рамках диссертационного исследования на вопрос: «Нужно ли следователям и судьям обладать знаниями о понятийном аппарате криптовалютной экосистемы и пониманием функционирования технологии блокчейн для расследования и рассмотрения уголовных дел о хищении криптовалюты?», ответили: «Да» (приложение 1).

Однако прежде следует определиться с тем, что такое криптовалютная экосистема. Изначально слово «экосистема» относится к природным объектам. Однако с развитием общественных отношений данное слово стало активно применяться и в других сферах жизнедеятельности. В частности, появилось словосочетание «цифровая экосистема», которое наиболее близко к теме диссертационного исследования. Под цифровой экосистемой понимают комплекс информационных систем, технологий, IT-продуктов и сервисов, взаимодействующих между собой и образующих единую сеть.[3] По аналогии с

[3] Казова З.М., Иванов З.А., Татаров Т.К., Шабатуков И.А., Шугушхов С.З. Цифровые экосистемы // Инновационная экономика: информация, аналитика, прогнозы. 2024. № 2. С. 124.

вышеуказанным определением предлагаем обозначить криптовалютную экосистему как комплекс блокчейн-технологий, предназначенных для взаимодействия с криптовалютой, на основе которых созданы все взаимосвязанные между собой элементы (криптовалюта, децентрализованные приложения и т.д.), а также организаций, разрабатывающих и совершенствующих блокчейн-технологии, предназначенные для взаимодействия с криптовалютой, и оказывающих услуги, облегчающие взаимодействие с криптовалютой.

С появлением и развитием криптовалютной экосистемы возник его собственный понятийный аппарат. В данном диссертационном исследовании мы затронем необходимую для предварительного расследования часть понятийного аппарата криптовалютной экосистемы.

Основополагающей технологией, лежащей в основе криптовалюты, является блокчейн. Следует сразу оговориться, что предназначение блокчейна намного шире, но в данной работе мы будем употреблять этот термин именно в контексте взаимодействия с криптовалютой.

А.И. Савельев полагает, что блокчейн представляет собой «децентрализованную распределенную базу данных обо всех подтвержденных транзакциях, совершенных в отношении определенного актива, в основе функционирования которой лежат криптографические алгоритмы».[4]

Е.В. Былинкина опирается на дефиницию, данную в стандарте ISO 22739:2020 «Технологии блокчейн и распределенного реестра. Словарь», где блокчейн определяется в качестве распределенного реестра с подтвержденными блоками, организованными в последовательную цепочку только для добавления с использованием криптографических ссылок, предлагая альтернативное определение: «Блокчейн есть разновидность распределенного реестра, предназначенного только для добавления

[4] Савельев А.И. Некоторые правовые аспекты использования смарт-контрактов и блокчейн-технологий по российскому праву // Закон. 2017. № 5. [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 14.06.2024).

информации, данные в который записываются блоками с использованием криптографических алгоритмов таким образом, что каждый новый блок включает информацию о предыдущем блоке. Безопасность данных в блокчейне обеспечивается за счет децентрализованного хранения информации и применения криптографических алгоритмов».[5]

В.А. Вайпан обозначает блокчейн в качестве «сквозной цифровой технологии, явления экономической жизни», требующего нового нормативного правового регулирования.[6]

Отметим, что блокчейн может быть предназначен не только для взаимодействия с криптовалютой, но и для работы в других сферах деятельности. В данной работе блокчейн будет рассмотрен как технология, благодаря которой стало возможно существование криптовалюты и взаимодействие с ней.

Слово блокчейн состоит из двух английских слов: «block», означающее «блок» и «chain», означающее «цепь». То есть, буквально, блокчейн означает цепь блоков. Название соответствует тому, как устроены транзакции в блокчейне.

Перед тем, как продолжить далее, считаем необходимым отвлечься на определение транзакции, поскольку может сложиться впечатление, что это только перевод криптовалюты из одного адреса на другой. Под транзакцией следует понимать любое действие пользователя с криптовалютой, как, например, перевод, обмен, перевод с помощью моста (децентрализованного приложения), предоставление децентрализованному приложению разрешения распоряжаться средствами на кошельке, предоставление ликвидности бирже, отправка криптовалюты на депозит, использование ее в качестве залога, заем,

---

[5] Былинкина Е.В. Блокчейн: правовое регулирование и стандартизация // Право и политика. 2020. № 9. С. 143-155. [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 12.08.2024).

[6] Вайпан В.А. Основы правового регулирования цифровой экономики // Право и экономика. 2017. № 11. С. 5-18. [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 11.09.2024).

отправка в стейкинг и другие действия. За любое из этих действий необходима оплата комиссии в основной криптовалюте блокчейна.

Инициированная транзакция в блокчейне не сразу доходит до своего получателя, а сначала попадает в мемпул (или memory pool), где находятся все инициированные транзакции в ожидании обработки лицами, которые являются майнерами или валидаторами блокчейна. Майнеры или валидаторы посредством своих ресурсов отбирают транзакции для обработки в отдельный список, который называется блоком. После того, как в данном списке заканчивается место или время для формирования, майнеры или валидаторы закрепляют данный блок в блокчейне, как самый последний, после чего все транзакции в блоке доходят до своих получателей, а майнеры или валидаторы начинают отбор следующих транзакций для формирования следующего блока в цепи. При этом каждый новый блок включает информацию о предыдущем блоке. Данные о совершенных транзакциях хранятся не на одном сервере, а у всех майнеров или валидаторов. По этой причине фальсификация информации о транзакциях крайне затруднительна.

Блокчейн имеет три взаимосвязанные составляющие:

1. Механизм консенсуса и валидации;
2. Механизм вознаграждения майнеров или валидаторов;
3. Криптовалюта.

Механизм консенсуса и валидации – это внутреннее устройство блокчейна, которое определяет то, какие транзакции являются действительными, а какие таковыми не являются. Данный механизм заложен в программный код блокчейна и все майнеры или валидаторы работают по этому механизму. Для того, чтобы транзакция оказалась записанной в блокчейн, необходимо, чтобы несколько майнеров или валидаторов подтвердили ее подлинность. На сегодняшний день существует два наиболее часто используемых механизма консенсуса и валидации – это «Proof of work» и «Proof of stake».

«Proof of work» дословно переводится, как «доказательство работы».

Это механизм работы блокчейна, при котором для поддержания его работы осуществляется майнинг, то есть деятельность по проведению математических вычислений путем эксплуатации технических и программно-аппаратных средств для внесения записей в информационную систему, использующую технологию, в том числе технологию распределенного реестра, имеющих целью выпуск цифровой валюты и (или) получение лицом, осуществляющим такую деятельность, вознаграждения в цифровой валюте за подтверждение записей в информационной системе.[7] То лицо или группа лиц (майнинг-пул), чье оборудование создаст новый блок первым, получит вознаграждение от блокчейна (в результате эмиссии новых единиц криптовалюты). Те майнеры, чье оборудование подтвердит транзакции, получит вознаграждение в качестве комиссий от инициаторов транзакций. Награды распределяются соразмерно предоставленной вычислительной мощности оборудования, если в майнинге участвует группа лиц (майнинг-пул). Именно вознаграждение является основной причиной заинтересованности майнеров в том, чтобы нести расходы на приобретение и использование вычислительных мощностей. Более того, майнеры постоянно конкурируют между собой в увеличении вычислительных мощностей, чтобы увеличить вероятность добычи криптовалюты, а именно, приобретают специализированное оборудование с более высоким уровнем вычислительной мощности или увеличивают количество своего оборудования, предназначенного для майнинга.

«Proof of stake» дословно переводится, как «доказательство доли». Это механизм работы блокчейна, при котором в качестве подтверждения транзакций осуществляется валидирование транзакций лицом или группой лиц, которые должны соответствовать определенным критериям (например,

[7] Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 04.12.2025).

иметь определенное количество конкретной криптовалюты на определенном блокчейне). Данных лиц принято называть валидаторами. Суть их работы заключается в «заморозке» имеющейся у них криптовалюты, а также в настройке технического и программно-аппаратного средства, называемого узлом или нодой (от английского слова «node», означающего «узел»), которое подключается к блокчейну и совместно с замороженной криптовалютой участвует в валидации транзакций. Валидаторы могут получать награду от блокчейна (в результате эмиссии новых единиц криптовалюты), от инициаторов транзакций в виде комиссий, а также в результате фиксированной доходности на свою замороженную криптовалюту. Деятельность по валидации транзакций называется стейкингом.

Исходя из изложенного, на наш взгляд, блокчейн следует определить, как распределенную базу данных обо всех подтвержденных транзакциях, функционирование и безопасность которой обеспечивается механизмами консенсуса и валидации, а также вознаграждения майнеров или валидаторов. Данное определение подходит именно для тех блокчейнов, которые подразумевают взаимодействие с криптовалютой.

Наиболее точное, на наш взгляд, определение дает Л.В. Бертовский, определяя блокчейн как распределенную базу данных, у которой устройства хранения данных не подключены к общему серверу. Эта база данных хранит постоянно растущий список упорядоченных записей, называемых блоками. Каждый блок содержит метку времени и ссылку на предыдущий блок. Чаще всего копии цепочек блоков хранятся и независимо друг от друга обрабатываются на разных компьютерах. Основным принципом функционирования новой технологии является прозрачность совершаемых операций с невозможностью их изменения лицами, не имеющими к ней санкционированного доступа.[8]

[8] Бертовский Л.В. Технология блокчейна в уголовном процессе как элемент цифрового судопроизводства // Проблемы экономики и юридической практики. 2017. № 6. С. 228.

В каждом блокчейне существует один или несколько видов криптовалюты, у которых имеются свои наименования (тикеры), идентификаторы и рыночные цены, если криптовалюта прошла процедуру допуска на биржу. Одна из нескольких криптовалют (или единственная криптовалюта) в блокчейне является основной. Это означает, что именно в данной криптовалюте необходимо производить оплату комиссий для осуществления транзакций. В разных блокчейнах может быть разное количество криптовалюты, которое закладывается на уровне программного кода. Данное количество может быть фиксированным, либо имеется возможность увеличить и (или) уменьшить ее количество. Также на уровне программного кода по-разному может быть урегулирован размер вознаграждения майнеров или валидаторов. Кроме криптовалюты, на блокчейне могут быть размещены децентрализованные приложения, состоящие из смарт-контрактов, к рассмотрению которых мы вернемся позже.

Так, например, работа блокчейна «Bitcoin» функционирует на механизме консенсуса Proof of work (доказательство работы). В данном блокчейне учет балансов осуществляется при помощи криптовалюты биткоин с сокращенным названием (тикером) BTC. Количество BTC фиксировано и равно 21 миллиону. BTC может делиться на более мелкое значение (например, 0,00000001 BTC). Майнеры получают награду за подтверждение транзакций в комиссиях, которые уплачиваются инициаторами транзакций, а также за счет эмиссии криптовалюты блокчейном «Bitcoin» за формирование каждого последующего блока транзакций.

Из вышеизложенного, для целей предварительного расследования важно понимать, что криптовалюта не может существовать без блокчейна, функционирование и безопасность которого должна поддерживаться майнерами или валидаторами. Эти знания позволят следователю (дознавателю) разграничить хищение криптовалюты от хищения активов, которые не являются криптовалютой. Проведя такое разграничение, появится понимание того, к какой методике расследования и тактике проведения

отдельных следственных действий необходимо прибегнуть.

В завершение разбора того, что из себя представляет блокчейн, важно отметить, что история транзакций на большинстве блокчейнов доступна всем пользователям и актуализируется по мере совершения новых транзакций. Исключением являются анонимные блокчейны, осмотр которых не дает объективных данных о совершенных транзакциях.

Благодаря вышеуказанному свойству возможно отследить любые транзакции в блокчейн-обозревателях, которые представляют собой сайт в сети Интернет. У каждого блокчейна имеется такой обозреватель. Так, например, у блокчейна «Arbitrum One» блокчейн-обозреватель имеет URL адрес https://arbiscan.io/.

Данная возможность крайне важна для предварительного расследования, поскольку благодаря ее использованию возможно получить объективную информацию о совершенных транзакциях, как, например, ID транзакции (идентификатор транзакции), дата, точное время, размер переведенных средств, публичные адреса (ключи) криптовалютных кошельков отправителей и получателей и другую, имеющую значение, информацию.

По нашему мнению, для успешного расследования хищений криптовалюты, важно знать о способах, используемых для доступа к криптовалюте, и инструментах, предназначенных для получения доступа к ней.

Любая криптовалюта хранится в блокчейне и существовать вне блокчейна не может. Получение доступа к криптовалюте осуществляется пользователями с помощью криптовалютного кошелька.

По мнению Д.И. Шнейдеровой криптовалютный кошелек – это инструмент, позволяющий хранить публичные и приватные ключи, ID транзакций, переводить, получать, обменивать криптовалюты, взаимодействовать с децентрализованными приложениями, непосредственный осмотр которого позволит установить наличие или отсутствие на нем криптовалютных активов; публичные и приватные ключи;

совершенные с данного кошелька транзакции и их характер; время их проведения; статус их подтверждения; количество криптовалюты, с которой совершены транзакции; публичные адреса кошельков, в адрес которых совершены транзакции; публичные адреса кошельков, с которых совершены транзакции в адрес осматриваемого кошелька, а также другую информацию, касающуюся взаимодействий с другими кошельками и децентрализованными приложениями.[9]

А.М. Чихрадзе определил криптовалютный кошелек как программное обеспечение или аппаратное устройство, предназначенное для хранения, отправки и получения криптовалют.[10]

Необходимо внести некоторую ясность. Криптовалютный кошелек не может быть привязан к адресу электронной почты, номеру телефона и другим данным. Эти данные используются для регистрации аккаунта на централизованной бирже, где пользователь может осуществлять операции с криптовалютой. При регистрации аккаунта централизованная биржа выделяет для пользователей криптовалютный кошелек, но он принадлежит не пользователям, а централизованной бирже. Каждому из пользователей присваивается уникальный ID для идентификации, и каждый пользователь видит только свой собственный баланс через интерфейс биржи.

Для создания криптовалютного кошелька не нужно указывать такие данные, как, например, номер телефона, адрес электронной почты, фамилия, имя и отчество. Доступ к криптовалютному кошельку обеспечивается с помощью мнемонической фразы или приватного ключа.

---

[9] Шнейдерова Д.И. Осмотр онлайн-криптокошелька заявителя/потерпевшего (по материалам и уголовным делам о хищениях в сфере оборота криптовалют): процессуальный и криминалистический аспекты // Алтайский юридический вестник № 4 (40) 2022 г. С. 157.

[10] Чихрадзе А.М. Семантика криптовалютной экосистемы: вызовы для криминалистической терминологии // Российский следователь. 2025. № 6. С. 14-18. [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 10.11.2025).

Отсутствие привязки к личности создает ряд трудностей для предварительного расследования. Однако следует иметь ввиду, что криптовалюта представляет собой ценность, которую возможно приобрести в обмен на национальную валюту и, наоборот, криптовалюта может быть обменена на национальную валюту. Наиболее часто встречающийся способ обмена подразумевает банковский перевод безналичных денежных средств на банковские счета лиц, которые осуществляют деятельность по обмену криптовалюты на национальную валюту и наоборот. Эти лица принято называть криптовалютными обменниками. Вышеуказанное означает, что, проведя ряд оперативно-розыскных мероприятий и следственных действий, есть вероятность установить лиц, с чьих банковских счетов произведен перевод денежных средств и на чьи счета поступили денежные средства в обмен на криптовалюту.

Также следует отметить, что криптовалютный кошелек предназначен не для хранения криптовалюты, а для воспроизведения информации о балансах криптовалют на одном или нескольких блокчейнах. Криптовалюта хранится в блокчейне. Однако в целях экономии текста мы будем употреблять словосочетание «способ хранения криптовалюты». Так как многие привыкли думать, что криптовалютный кошелек хранит криптовалюту, существует распространенное заблуждение, что если криптовалютный кошелек создан с помощью конкретного программного обеспечения, то доступ к этому кошельку возможен только через это программное обеспечение. Поэтому важно уточнить, что программное обеспечение, являющееся криптовалютным кошельком – это, всего лишь, интерфейс, с помощью которого возможно просмотреть наличие или отсутствие криптовалюты на балансе, совершать транзакции и другие действия. Любой криптовалютный кошелек возможно воспроизвести на любом программном обеспечении, выполняющим функции криптовалютного кошелька. Так, например, если кошелек был создан при помощи программы «Metamask», его возможно импортировать, используя любую другую программу, например, «OKX Wallet». Для этого необходимо

использовать мнемоническую фразу или приватный ключ. В результате такой импортации будет получен доступ к криптовалюте через программное обеспечение «OKX Wallet».

Эта информация полезна для эффективной организации предварительного расследования, поскольку, в некоторых ситуациях, производство осмотра криптовалютного кошелька целесообразно через конкретное программное обеспечение, так как оно имеет необходимый функционал, который необходимо задействовать при осмотре.

Исходя из изложенного, предлагаем дать следующее определение криптовалютному кошельку. Криптовалютный кошелек – это программное обеспечение или аппаратное устройство, позволяющее воспроизвести информацию о балансах криптовалют на блокчейнах, получать и отправлять криптовалюту, а также совершать с ней иные действия.

Криптовалютные кошельки возможно классифицировать по разным признакам, однако для предварительного расследования видим целесообразным классифицировать по трем:

1. В зависимости от подключения к сети Интернет (горячие и холодные);

2. В зависимости от типа хранения мнемонической фразы и приватных ключей (кастодиальные и некастодиальные);

3. В зависимости от того, с одним или несколькими блокчейнами поддерживают работу (одновалютные и мультивалютные).

Горячий криптовалютный кошелек представляет собой компьютерную программу, браузерное расширение, приложение на смартфоне или сайт централизованной биржи в сети Интернет. Взаимодействие с таким кошельком возможно только при наличии подключения к сети Интернет. Кроме того, приватные ключи этого кошелька хранятся на том устройстве, на которое установлено программное обеспечение (кроме сайта централизованной биржи).

Холодный криптовалютный кошелек представляет собой физически осязаемое устройство, воспроизведя которое возможно получить доступ к

активам. Он может быть в виде флеш-накопителя, пластиковой карты или другого аппаратного устройства, благодаря чему возможно взаимодействие с кошельком в оффлайн среде. Приватные ключи от кошелька хранятся на этом же устройстве. Мнемоническая фраза, как правило, демонстрируется для пользователя при первом воспроизведении кошелька.

Кастодиальным криптовалютным кошельком является такой кошелек, мнемоническая фраза и приватные ключи от которого хранятся у организации, которая оказывает желающим лицам комплекс различных услуг, связанных с торговлей криптовалютой, в числе которых предоставление криптовалютного кошелька во владение и пользование. Также организация предоставляет возможность обменивать национальную валюту на криптовалюту и наоборот при помощи peer-to-peer сервиса. Такую организацию принято называть централизованной биржей. Средства на таком кошельке не находятся под полным контролем и управлением собственника.

Для предварительного расследования данное понимание очень важно. Если кошелек принадлежит централизованной бирже и при этом невозможно установить ряд обстоятельств, имеющих значение для уголовного дела (например, осмотреть историю транзакций, совершенных с конкретного аккаунта по причине незнания пароля) путем проведения осмотров, обысков, выемок и допросов, есть шансы истребовать необходимую информацию и документы у централизованной биржи (особенно, если данная организация зарегистрирована на территории Российской Федерации). Также следует отметить, что для регистрации аккаунта на централизованной бирже необходимо указать персональные данные. Большинство централизованных бирж требуют прохождение верификации личности (KYC) по документу, удостоверяющему личность или содержащему персональные данные конкретного физического лица.

Некастодиальным криптовалютным кошельком является такой кошелек, мнемоническая фраза и приватные ключи от которого предоставляются только

тому лицу, которое создало кошелек. Средства на таком кошельке находятся под полным контролем и управлением собственника.

Для предварительного расследования это означает, что отследить историю транзакций возможно только если есть доступ к криптовалютному кошельку, либо если имеется информация о публичном адресе кошелька или хэше транзакции (ID транзакции). Запросить информацию у третьих лиц возможности нет.

Одновалютные кошельки поддерживают работу только с одним блокчейном. Это означает, что если воспроизвести криптовалютный кошелек через программное обеспечение, выполняющее функцию одновалютного кошелька, то будет получен доступ только к тем криптовалютам, которые размещены на одном конкретном блокчейне, который доступен для работы. Так, например, взаимодействуя с программным обеспечением «Petra Wallet», будет доступен только блокчейн «Aptos» и все криптовалюты, которые размещены на данном блокчейне. Криптовалюты и истории транзакций других блокчейнов при помощи такого программного обеспечения обозреть невозможно, но это не означает, что их нет.

Данная информация также важна для полного и всестороннего предварительного расследования, а также проверки собранных доказательств. Если нужен доступ к истории транзакций на другом блокчейне, необходимо воспроизвести этот кошелек при помощи мнемонической фразы на другом программном обеспечении, которое поддерживает работу с нужными блокчейнами.

Мультивалютные кошельки поддерживают работу с несколькими или с большим количеством разных блокчейнов. Однако следует исходить из того, что нет такого программного обеспечения, которое поддерживало бы работу со всеми существующими блокчейнами, поскольку, со временем, разрабатываются новые блокчейны, работу которых, в первое время, поддерживают одновалютные кошельки, разработанные создателями новых блокчейнов.

В предыдущих абзацах было упомянуто про публичный адрес (ключ), приватный ключ и мнемоническую фразу, являющиеся неотъемлемой частью знаний, которой необходимо обладать для эффективного расследования хищений криптовалют. По этой причине следует дать определения всему вышеуказанному, а также пояснить, какую роль они играют как при взаимодействии с криптовалютой, так и при расследовании хищений криптовалюты.

Публичный адрес (ключ) – это адрес криптовалютного кошелька, представляющий собой уникальный набор латинских букв и цифр, зная который возможно произвести перевод криптовалюты в адрес этого кошелька, просмотреть его баланс, историю всех транзакций, а также историю всех поступлений с помощью блокчейн-обозревателя. Если привести аналогию, то это то же самое, что номер расчетного счета в банке. Как правило, для каждой криптовалюты существует отдельный публичный адрес. Иногда может быть единый адрес для группы разных криптовалют в рамках одного блокчейна. Узнать публичный адрес возможно в ходе допроса (получения объяснения), если лицо продемонстрирует его со своего устройства, а также в ходе осмотра устройства, на котором установлено программное обеспечение, выполняющее функцию криптовалютного кошелька (если на этом программном обеспечении воспроизведен искомый кошелек). Для целей предварительного расследования публичный адрес необходим для осмотра и анализа с помощью блокчейн-обозревателя или программного обеспечения, выполняющего функцию криптовалютного кошелька, истории исходящих и входящих транзакций. Это позволит убедиться в существовании или отсутствии тех или иных фактов (например, наличии или отсутствии транзакции), выдвинуть следственные версии, а также организовать и спланировать последующие действия.

Важно понимать, если криптовалюта будет отправлена на неправильный или несуществующий публичный адрес, она будет утеряна навсегда. Знание данной информации также полезно, так как позволяет проверить версию об отсутствии факта хищения.

Приватный ключ – это скрытый от третьих лиц уникальный набор латинских букв и цифр, который позволяет получить доступ к конкретной криптовалюте или группе конкретных криптовалют, а также используется для подписания транзакций. Также обладая информацией о приватном ключе, возможно получить связанные с ним публичные адреса (но не наоборот), а также доступ к криптовалюте в рамках одного блокчейна. Получив такой доступ через криптовалютный кошелек, будет возможность осмотреть историю транзакций (если используемый криптовалютный кошелек имеет соответствующий функционал).

Мнемоническая фраза представляет собой набор слов в определенной последовательности, который позволяет воспроизвести все приватные ключи в программном обеспечении, являющемся криптовалютным кошельком. Она позволяет получить доступ ко всем средствам, хранящимся на всех блокчейнах, которые способно воспроизвести программное обеспечение, выполняющее функцию криптовалютного кошелька.

Значительная часть способов хищения криптовалюты направлена на получение злоумышленниками мнемонической фразы или приватных ключей.

Переходя к более подробному разбору криптовалюты, важно отметить, что она не является чем-то вещественным. Это лишь цифровая запись в распределенном реестре. То есть криптовалюта является методом учета балансов внутри блокчейна и, как было указано выше, вне блокчейна существовать не может.

В настоящее время существует ряд работ, посвященных сущности криптовалюты, где выделяют следующие ее свойства:

1. Это актив, который существует в цифровом виде или является цифровым представлением другого актива;
2. Существует деление оборота криптовалюты на централизованный и децентрализованный. При централизованном обороте существует администратор, который регулирует майнинг, реестр и вправе выводить криптовалюту из оборота. Децентрализованный оборот более распространен и

подразумевает хранение и распределение криптовалюты без централизованного участия, реестр проведенных операций хранится распределенно;

3. Данный актив не является средством расчета, используется в качестве виртуального платежного средства, не имея при этом правового статуса;

4. Обладает отдельными свойствами товарных и кредитных денег, но не в состоянии полноценно выполнять все функции денег, включает цифровые валюты в соответствии с Законом о ЦФА, а также цифровые финансовые активы, которые могут использоваться в иностранной юрисдикции для платежей;

5. Отсутствуют единый эмитент, выпуск, администратор, осуществляющий ее учет на счетах пользователей;

6. Отсутствуют гарантии защиты прав потребителей.[11]

Со всеми вышеуказанными выводами можно согласиться с одной лишь оговоркой о том, что майнинг – это не единственный механизм работы технологии блокчейн, как отмечалось ранее.

Криптовалюты также можно разделить на основную криптовалюту и токены. Основную криптовалюту блокчейна принято называть монетой и ее основное отличие заключается в том, что она является средством для уплаты комиссий за совершение транзакций. При отсутствии основной криптовалюты блокчейна в необходимом количестве, транзакции на некостадиальных кошельках совершить невозможно. На кастодиальных кошельках транзакцию совершить возможно, поскольку централизованная биржа уплачивает такую комиссию, а пользователь компенсирует централизованной бирже эти

[11] См. например: Гейкина И.В. Понятия цифровой валюты и криптовалюты, их отличия // Нотариальный вестник. 2023. № 7. С. 17-23, Безручко Е.В., Ходусов А.А. Преступления, совершаемые с использованием информационно-коммуникационных средств: философско-правовое конструирование эффективных классификаций // Философия права. 2020. № 3 (94). С. 89-95 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 10.11.2025).

расходы в той криптовалюте, в которой совершил транзакцию. Токен создается поверх существующего блокчейна при помощи смарт-контрактов, к разбору которых мы вернемся позже, и может иметь определенный функционал. Создание токена намного проще, поскольку создателям не нужно разрабатывать блокчейн. С токенами также возможно совершать транзакции (при уплате комиссии в основной криптовалюте). Токены можно разделить на определенные родовым признаком и индивидуально-определенные (NFT или невзаимозаменяемый токен). NFT, чаще всего, представляет собой токенизированное изображение, имеющее уникальный идентификатор (номер контракта). Два визуально одинаковых NFT являются разными токенами, так как имеют разные идентификаторы. Однако NFT может представлять собой не просто токенизированное изображение, а также выступать в качестве свидетельства о праве собственности.

Поскольку создание токена намного проще, чем создание основной криптовалюты, существует множество токенов, созданных с целью совершения хищений, под видом того, что они имеют какой-то полезный функционал или высокий потенциал роста в цене. Также нередко злоумышленники создают токены с тикерами, которые идентичны тикерам настоящих токенов, чтобы выдать их за настоящие.

Также следует отметить, что криптовалюта с одним и тем же тикером на разных блокчейнах может выступать в роли основной криптовалюты или токена. Так, например, монета ETH на блокчейне «Ethereum» - это основная криптовалюта, в которой необходимо уплачивать комиссию валидаторам для совершения транзакций. Однако ETH на блокчейне «Solana» - это токен. Для совершения транзакций в рамках данного блокчейна необходимы монеты SOL.

Любая криптовалюта имеет свой идентификатор (контракт), представляющий собой уникальный набор латинских букв и цифр. Для предварительного расследования это важно, поскольку необходимо корректно указывать предмет хищения в процессуальных документах, в частности, в

постановлении о привлечении лица в качестве обвиняемого и обвинительном заключении (акте или постановлении).

Криптовалюта с одним и тем же тикером и одинаковой рыночной ценой на разных блокчейнах – это две разные монеты, с точки зрения предмета хищения.

Возвращаясь к тому, что такое смарт-контракт, его можно определить, как программный код, изготовленный на блокчейне, и выполняющий набор команд по заданным условиям.

Существует мнение, что смарт-контракт является договором в электронной форме, исполнение прав и обязательств по которому осуществляется путем совершения в автоматическом порядке цифровых транзакций в распределенном реестре цифровых транзакций в строго определенной им последовательности и при наступлении определенных им обстоятельств.[12]

Также существует мнение, что смарт-контрактом называется компьютерная программа (или компьютерный код), которая может быть заключена только с использованием технологии блокчейн и позволяет автоматически заключать, исполнять и прекращать различные договоры в момент наступления заранее установленных юридических фактов.[13]

Вышеуказанное определение является более точным.

Поскольку смарт-контракт является программным кодом, он позволяет создавать не только токены на блокчейнах, а также различные приложения, которые принято называть децентрализованными приложениями. Децентрализованное приложение представляет собой сайт в сети Интернет, выполняющий определенный функционал, к которому возможно подключить

---

[12] Зенин С.С., Кутейников Д.Л., Ижаев О.А., Япрынцев И.М. Правотворчество в условиях алгоритмизации права // Lex russica. 2020. № 7 (164). С. 97-104. [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 10.06.2025).

[13] Ефимова Л.Г., Сиземова О.Б. Правовая природа смарт-контракта // Банковское право. 2019. № 1. С. 23-30. [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 10.06.2025).

некастодиальный кошелек и совершать те действия, для которых он предназначен. Это могут быть игры, маркетплейсы, децентрализованные биржи для обмена и торговли криптовалютой и т.д. Их особенность заключается в том, что нет необходимости регистрироваться, указывать персональные данные, а также то, что все действия реализуются в результате работы смарт-контрактов, без участия третьих лиц. Так, например, чтобы обменять одну криптовалюту на другую на централизованной бирже, помимо прохождения процедуры регистрации и верификации личности, необходимо совпадение двух заявок разных пользователей, которое организует централизованная биржа. Обмен криптовалюты на децентрализованной бирже не подразумевает регистрации и сведения двух заявок. Пользователь подключает свой некастодиальный кошелек к бирже, предоставляет разрешение бирже воспользоваться криптовалютой, указав лимиты или безлимитно, далее осуществляет обмен путем предоставления обмениваемой криптовалюты в пул ликвидности биржи и получает желаемую криптовалюту из этого же пула ликвидности благодаря работе смарт-контрактов. Злоумышленники активно пользуются возможностью анонимно создавать децентрализованные приложения, которые предназначены для совершения хищений криптовалютных активов. Введенные в заблуждение пользователи подключают свой криптовалютный кошелек к децентрализованному приложению и подтверждают какое-либо действие (то есть запускают в работу смарт-контракт), которое, на первый взгляд, не является подозрительным, но на самом деле, направлено на предоставление согласия на распоряжение криптовалютой или перевод криптовалюты на кошелек злоумышленника и т.д.

Знания о том, что такое смарт-контракт и децентрализованное приложение также важно для расследования. В ходе грамотно выстроенного допроса и (или) осмотра владеющим понятийным аппаратом следователем (дознавателем) появится возможность определить, при помощи какого децентрализованного приложения стало возможно хищение криптовалюты,

принадлежащей потерпевшему.[14]

1.2. Понятие криминалистической характеристики дистанционных хищений криптовалютных активов. Криптовалютные активы как предмет преступного посягательства

Не останавливаясь подробно на анализе понятия криминалистической характеристики преступлений, которому были посвящены труды многих криминалистов[15], мы присоединяемся к определению, изложенному Н.П. Яблоковым, что она представляет собой систему сведений, отражающую закономерные связи между отдельными элементами конкретного вида (группы) преступлений; сведений, совокупность которых позволяет получить следователю криминалистически значимую информацию для правильной организации процесса расследования.[16]

Исходя из данного определения криминалистическую характеристику хищений криптовалютных активов определим как систему криминалистически значимых знаний о составных элементах хищения криптовалютных активов, в которую входят предмет преступного

---

[14] Гайсин Н.И. К вопросу о необходимости криминалистического обеспечения расследования хищений криптовалютных активов // Вестник Института права Башкирского государственного университета. 2024. № 4(24). С. 160.

[15] См. например: Белкин Р.С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики / Р. С. Белкин. — М.: Издательство НОРМА (Издательская группа НОРМА–ИНФРА М), 2001. С. 223, Сергеев Л.А. Расследование и предупреждение хищений, совершаемых при производстве строительных работ: автореф. дис. … к-та юрид. наук. Москва, 1966. 16 с, Колесниченко А.Н. Научные и правовые основы расследования отдельных видов преступлений: автореф. дис. … д-ра юрид. наук. Харьков, 1967. С. 14, Бессонов А.А. Основы криминалистического учения об исследовании и использовании криминалистической характеристики преступлений. М.: Юрлитинформ, 2016. С. 129–133, Коновалова В.Е., Колесниченко А.Н. Теоретические проблемы криминалистической характеристики // Криминалистическая характеристика преступлений: сб. науч. тр. М., 1984. С. 16, Каневский Л.Л. Разработка типовых криминалистических характеристик преступлений и их использование в процессе расследования // Российский юридический журнал. 2000. № 2. С. 111, Бессонов А.А. Частная теория криминалистической характеристики преступлений: автореф. дис. … д-ра юрид. наук. Москва, 2017. С. 11, и др.

[16] Яблоков Н.П. Криминалистика: учеб. М., 2000. 371 с.

посягательства, способ хищения, личность преступника, механизм следообразования в виде электронных (цифровых) следов, а также личность потерпевшего, корреляционные связи между которыми представляют вероятностный вывод о личности преступника.

Одним из элементов криминалистической характеристики хищений криптовалюты следует обозначить предмет преступного посягательства. Долгое время вопрос о правовой природе криптовалюты являлся спорным, поскольку в Российской Федерации, как и во многих других государствах, не был закреплен ее правовой статус. По этой причине защита прав многих граждан не была обеспечена. Правоохранительные органы неоднократно отказывали в возбуждении уголовных дел по фактам совершенных хищений криптовалют, поскольку с правовой точки зрения отсутствовал необходимый элемент состава преступления – объект. Также имели место случаи, когда суды отказывались признавать виновными тех, кто совершил хищение криптовалюты. Следует отметить, что такие судебные акты отменялись или подвергались изменениям вышестоящими судами.[17] Однако на сегодняшний день данный пробел в действующем законодательстве восполнен. Согласно п. 1 ст. 1 Федерального закона от 29.11.2024 № 418-ФЗ «О внесении изменений в части первую и вторую Налогового кодекса Российской Федерации и отдельные законодательные акты Российской Федерации», цифровая валюта признается имуществом.[18] По этой причине мы можем сделать однозначный вывод о том, что криптовалюта или цифровой актив является предметом преступного посягательства.

Однако в вышеуказанном законодательном акте дословно закреплено, что имуществом признается не криптовалюта, а цифровая валюта. Кроме того,

---

[17] Апелляционное определение Санкт-Петербургского городского суда от 23.11.2020 № 22-5295/2020, 1-95/2020 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 01.06.2025).

[18] Федеральный закон от 29.11.2024 № 418-ФЗ «О внесении изменений в части первую и вторую Налогового кодекса Российской Федерации и отдельные законодательные акты Российской Федерации» [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 14.11.2025).

в Федеральном законе 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» нет слова «криптовалюта». Поэтому можно прийти к ошибочному выводу о том, что криптовалюта не может рассматриваться в качестве предмета преступного посягательства. Во избежание каких-либо сомнений о том, что криптовалюта является цифровой валютой, следует привести ряд убедительных аргументов:

1. В пояснительной записке к законопроекту № 1065710-7 «О внесении изменений в части первую и вторую Налогового кодекса Российской Федерации и отдельные законодательные акты Российской Федерации (в части налогообложения цифровой валюты) дословно указано «Масштабное распространение технологии «блокчейн» и расширение числа экономических субъектов, использующих криптовалюту, в том числе с целью получения доходов, требует законодательной определенности в части ее налогообложения.

Криптовалюта часто используется в целях уклонения от уплаты налогов, для легализации средств, добытых преступным путем, и финансирования противоправной деятельности».[19]

Исходя из текста пояснительной записки очевидно, законодатель не скрывает, что криптовалюта является цифровой валютой в контексте Федерального закона от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», которую признали имуществом, в первую очередь, из-за масштабного распространения использования криптовалюты.

[19] Пояснительная записка к законопроекту № 1065710-7 «О внесении изменений в части первую и вторую Налогового кодекса Российской Федерации и отдельные законодательные акты Российской Федерации (в части налогообложения цифровой валюты)» [Электронный ресурс] // Система обеспечения законодательной деятельности Государственной автоматизированной системы «Законотворчество» (СОЗД ГАС «Законотворчество») : сайт. URL: https://sozd.duma.gov.ru/download/2a8393c0-0964-4237-9867-36a6e01f1cd5 (дата обращения: 27.09.2025).

По нашему мнению, если криптовалюта является имуществом и облагается налогом, то ее собственник вправе обратиться в правоохранительные органы в случае ее хищения.

2. Анализ практики вышестоящих судов подтверждает, что криптовалюта является цифровой валютой. Ярким примером является кассационное определение Третьего кассационного суда общей юрисдикции от 24.06.2021 № 77-1411/2021, в котором непризнание нижестоящими судами криптовалюты, как объекта преступного посягательства, приравнено к существенному нарушению норм уголовного права, повлиявшему на исход дела. Суд отнес похищенную криптовалюту к цифровой валюте, а также отменил нижестоящие судебные акты, в которых исключили из объема обвинения указания на незаконное завладение осужденными криптовалютой. Также существуют аналогичные судебные акты.[20]

Судебная коллегия по уголовным делам Верховного Суда Российской Федерации в своем кассационном определении от 15.11.2023 № 88-УДП23-7-К8 также выразила мнение относительно того, может ли криптовалюта являться объектом хищения: «Отсутствие законодательной определенности правового статуса «биткоинов» не свидетельствует об отсутствии материального ущерба…».[21]

3. Дополнительно следует отметить о существовании законопроекта № 902782-8 «О внесении изменений в статью 104-1 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» (об особенностях изъятия цифровой валюты), принятого в первом чтении. В пояснительной записке данного законопроекта упоминается о

[20] См. например: определение Первого кассационного суда общей юрисдикции от 20.08.2025 № 77-2652/2025, определение Третьего кассационного суда общей юрисдикции от 24.06.2021 № 77-1411/2021, кассационное определение Восьмого кассационного суда общей юрисдикции от 21.12.2023 № 77-5316/2023 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 27.09.2025).

[21] Кассационное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 15.11.2023 № 88-УДП23-7-К8 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 27.09.2025).

«криптобирже»[22], как способе хранения цифровой валюты, в связи с чем нет никаких сомнений в том, что законодатель под цифровой валютой подразумевал криптовалюту, а законопроект инициирован для законодательного закрепления порядка изъятия криптовалютных кошельков.

4. Федеральным законом от 08.08.2024 № 221-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации»[23] в Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» внесены поправки, в числе которых введено понятие «майнинг», являющееся способом поддержания работы блокчейна и добычи эмитируемой им цифровой валюты (криптовалюты).

Также следует добавить, что результаты опроса респондентов в рамках диссертационного исследования показали, что 100% респондентов считают, что криптовалюта может быть предметом преступного посягательства (приложение № 1).

Криптовалюта или цифровой актив не является чем-либо овеществленным. Поэтому следует разобраться, что именно является предметом преступного посягательства. Раскрывая содержание данного элемента более подробно, необходимо отметить, что действия злоумышленника нацелены на то, чтобы в конкретном блокчейне изменилась информация о количестве криптовалюты на кошельке потерпевшего в сторону уменьшения, а также на кошельке злоумышленника в сторону увеличения,

---

[22] Пояснительная записка к законопроекту № 902782-8 «О внесении изменений в статью 104-1 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации (об особенностях изъятия цифровой валюты)» [Электронный ресурс] // Система обеспечения законодательной деятельности Государственной автоматизированной системы «Законотворчество» (СОЗД ГАС «Законотворчество») : сайт. URL: https://sozd.duma.gov.ru/download/1f024e33-8bca-6002-84de-5501bb89ade0 (дата обращения: 27.09.2025).

[23] Федеральный закон от 08.08.2024 № 221-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 04.12.2025).

путем совершения комплекса различных действий, в большинстве случаев, всеми вышеперечисленными лицами или только злоумышленником. Таким образом, предметом преступного посягательства, буквально, является такое изменение информации в блокчейне о количестве криптовалюты на кошельке злоумышленника в сторону увеличения, которое было совершено собственником криптовалюты под влиянием обмана, либо путем злоупотребления его доверием, либо которое было совершено злоумышленником тайно от собственника. В результате такого изменения информации злоумышленник получает возможность владеть, пользоваться и распоряжаться криптовалютой, а в блокчейне происходит изменение информации о количестве криптовалюты на кошельке у собственника в сторону уменьшения, чем последнему причиняется ущерб.

1.3. Характеристика способов дистанционного хищения криптовалютных активов как системообразующий элемент криминалистической характеристики

Основным элементом криминалистической характеристики любого преступления является способ его совершения. Категория «способ совершения преступления» имеет междисциплинарный характер, при этом криминалистическое его понимание отличается от уголовно-правового, поскольку связано не с квалификацией преступления и определением степени его общественной опасности, а с поиском наиболее эффективных средств и методов его выявления, раскрытия и расследования.[24]

Анализ возможных способов совершения хищений криптовалюты представляется крайне важным как с теоретической, так и с практической точки зрения. Обладая знаниями о способах совершения хищений криптовалютных активов и их технических особенностях, следователи

[24] Васильев А.Н., Яблоков Н.П. Предмет, система и теоретические основы криминалистики. М., 1984. С. 118.

(дознаватели) будут производить допросы, осмотры и другие следственные действия наиболее эффективно, смогут выдвигать типичные следственные версии относительно способа совершения такого хищения, а также круга лиц, которые могли совершить данное преступление, и исходя из выдвинутых версий, оценивать благоприятность следственной ситуации, планировать дальнейшие действия.

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

Следует отметить дискуссионный характер теоретической возможности квалификации хищения криптовалюты, а также безналичных средств, как кражи. Развитие технологий обусловливает объективную необходимость совершенствования нормативного регулирования. В этом контексте применение статьи 158 УК РФ для квалификации хищений, совершаемых в цифровой сфере, некоторые исследователи считают архаичным, предлагая изменить законодательство.[25] Принимая во внимание несовершенство нормотворчества и наличие инициатив по его совершенствованию, в рамках

[25] См.: Вяткин, А. Н. Предложения по изменению законодательства для повышения эффективности оперативно-разыскной деятельности в борьбе с киберпреступностью / А. Н. Вяткин // Криминалистическая тактика: история, современное состояние и перспективы развития (к 85-летию со дня рождения профессора В. И. Комиссарова): материалы Международной научно-практической конференции, Москва, 14 марта 2024 года. – Москва: Проспект, 2024. – С. 51-54, Вяткин, А. Н. Проблемы противодействия киберхищениям и пути их решения / А. Н. Вяткин // Право и инновации: новые вызовы технологической революции: Материалы II Приволжского юридического конгресса, Уфа, 21 октября 2022 года. – Уфа: Научно-исследовательский институт проблем правового государства, 2022. – С. 36-44, Вяткин, А. Н. ОРД против киберпреступности: обеспечена ли оперативность? / А. Н. Вяткин // Высокотехнологичное право: современные вызовы: Материалы IV Международной межвузовской научно-практической конференции, Москва-Красноярск, 17–20 февраля 2023 года. Том Часть 2. – Красноярск: Красноярский государственный аграрный университет, 2023. – С. 29-33.

настоящего исследования мы ориентируемся на действующее законодательство и складывающуюся практику правоприменения.

Исходя из ответов на вопросы респондентов, в чьих производствах находились соответствующие уголовные дела (27%), 62% ответили, что хищение произошло в результате перевода криптовалюты потерпевшим в адрес злоумышленника, 29% - в результате получения злоумышленником доступа к криптовалютному кошельку, 9% - в результате предоставления вредоносному децентрализованному приложению разрешения на распоряжение криптовалютой (приложение 1).

Одним из самых распространенных способов хищения криптовалютных активов является фишинг. Использование данного способа характерно не только для хищения криптовалюты, но и безналичных денежных средств. В криптовалютной сфере фишинг заключается в том, что злоумышленник создает поддельные сайты, приложения, расширения для браузера или иное программное обеспечение, которые направлены на аккумулирование логинов, паролей, приватных ключей и мнемонических фраз от кошельков тех лиц, которые ввиду собственной неосмотрительности или незнанию основ безопасности при работе с криптовалютой передали вышеуказанную информацию, осуществив ее ввод в фишинговое программное обеспечение. Также создаются вредоносные децентрализованные приложения и смарт-контракты, при взаимодействии с которыми пользователи подписывают вредоносные транзакции.

Сайты, приложения, расширения для браузера и иное программное обеспечение очень похожи на официальные сайты, приложения, расширения для браузера и программное обеспечение, которые действительно предназначены для взаимодействия с криптовалютой.

Например, злоумышленник может создать сайт, который похож по дизайну и URL-адресу на официальный сайт централизованной криптовалютной биржи, где возможно производить различные манипуляции с криптовалютой. Адрес сайта, как правило, отличается от оригинального

одним символом. Например, вместо https://blockchain.com – https://blockcnain.com. Такой способ хищения рассчитан на невнимательность пользователей или их неопытность в использовании сети Интернет. После того, как пользователь осуществит ввод своих данных для получения доступа к аккаунту на поддельном сайте, злоумышленник сможет получить доступ к аккаунту пользователя и всем имеющимся на нем криптовалютным активам, которыми он сможет распорядиться по собственному усмотрению.[26] В приведенном нами примере суд признал подсудимого виновным в совершении преступления, предусмотренного ст. 159.6 УК РФ. Однако мы считаем, что действия осужденного подпадают под признаки, предусмотренные ст. 158 УК РФ, так как в приговоре указано, что он лишь получал данные для входа путем использования вредоносного программного обеспечения, подменяющего (модифицирующего) URL адрес сайта. При этом действия, направленные на перевод чужой криптовалюты, преступник совершал самостоятельно в результате незаконного получения и использования входных данных. Таким образом, модификация компьютерной информации не находится в прямой причинно-следственной связи с хищением криптовалюты. Кроме того, осужденный не взаимодействовал с лицами, у которых похитил криптовалюту, а они не осуществляли перевод своей криптовалюты в адрес осужденного.

Аналогичным примером является фишинг браузерных расширений или приложений. Злоумышленник создает браузерные расширения или приложения с таким же интерфейсом как, например, у криптовалютного кошелька. Основная цель заключается в получении от пользователя его мнемонической фразы, которой достаточно, чтобы получить доступ к кошельку и управлению всеми средствами, которые отображаются на нем.

Что касается фишинга децентрализованных приложений,

[26] Приговор Дорогомиловского районного суда города Москвы от 10.04.2024 по делу № 1-34/2024 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 15.08.2024).

злоумышленники активно пользуются возможностью анонимно создавать и размещать на блокчейне вредоносные децентрализованные приложения, которые внешне не отличаются от обычных, кроме URL адреса. К примеру, существует децентрализованная биржа для совершения обменов одной криптовалюты на другую с URL адресом https://app.uniswap.org. Поддельная децентрализованная биржа имеет почти незаметное отличие – https://app.uniswop.org. Введенные в заблуждение пользователи подключают свои некастодиальные кошельки к фишинговому децентрализованному приложению и подтверждают какое-либо действие, которое направлено на разрешение децентрализованному приложению распоряжаться криптовалютой на кошельке, либо перевод криптовалюты в адрес злоумышленника. При этом пользователь может не понять того, какое действие он совершил, либо думать, что совершил приемлемое для себя действие, поскольку данные о совершаемой транзакции могут быть умышленно подменены через отображаемый на устройстве интерфейс.

Следующий способ хищения криптовалютных активов, который хотелось бы упомянуть, заключается в использовании вредоносных программ. Для реализации данного способа необходимо, чтобы вредоносная программа оказалось на устройстве, где хранятся данные, позволяющие совершить хищение криптовалюты, либо способствующие такому хищению. Такое программное обеспечение может быть загружено пользователем как под влиянием обмана или злоупотребления доверием, либо без такового.

Как пример, пользователь под влиянием обмана загружает на свое устройство вредоносное программное обеспечение, функция которого заключается в получении данных криптовалютных кошельков или в подмене публичного ключа в буфере обмена. В момент, когда пользователь собирается произвести перевод криптовалюты на чей-либо публичный адрес, он должен скопировать публичный адрес, на который планируется перевод, в буфер обмена своего устройства. В момент вставки вредоносное программное обеспечение производит подмену скопированного публичного адреса на

публичный адрес злоумышленника. В результате пользователь переводит криптовалюту на публичный адрес злоумышленника. Заметить подмену адресов затруднительно, поскольку адрес представляет собой достаточно длинный набор латинских букв и цифр.

Еще одним способом хищения криптовалютных активов является подмена SIM-карты на устройстве, где хранятся данные для входа в личный кабинет пользователя централизованной криптовалютной биржи. В большинстве случаев для заведения кошелька на централизованной криптовалютной бирже необходима регистрация, для которой необходим номер телефона. На номер телефона, который был использован для регистрации, поступают коды при необходимости восстановления пароля от личного кабинета. Подменив SIM-карту, злоумышленник сможет получить доступ к аккаунту пользователя, сменив пароль с помощью функции восстановления пароля через SMS-сообщения.

Отдельно следует выделить хищения, совершенные в результате хакерской атаки. Для совершения таких хищений необходимы специальные познания, а в некоторых случаях и доступы к исходным кодам, например, в силу выполняемых должностных обязанностей. Ввиду специфичности этого способа, нет возможности подробно описать механизмы таких хищений. Единственное, что объединяет такие хищения – это использование уязвимостей в программных кодах. В результате эксплуатации уязвимостей злоумышленник получает приватные ключи от криптовалютных кошельков, либо похищает средства из пулов ликвидности децентрализованных приложений, совершив вредоносные транзакции. Такие транзакции не соответствуют логике, которая закладывалась в смарт-контракты, при их изготовлении, как на программном уровне, так и на уровне здравого смысла. То есть, эксплуатируя уязвимость при совершении обмена криптовалют, злоумышленник имеет возможность получить несоразмерно больше средств, чем должен был. Примером является хищение криптовалюты из пулов

ликвидности децентрализованной биржи «Cetus» на блокчейне «SUI».[27]

Существует также множество способов хищения, когда пользователи сами осуществляют перевод своих активов на чужие публичные адреса. Злоумышленники используют множество разных способов, чтобы войти в доверие и (или) ввести пользователей в заблуждение.

Для примера приведем один из таких способов. Некоторые пользователи желают обменять свою криптовалюту на национальную валюту. Сделать это возможно при помощи peer-to-peer сервиса на централизованной бирже. Пользователь, который желает продать криптовалюту, переводит ее на публичный адрес, указанный в заявке покупателя криптовалюты, а пользователь, который желает купить криптовалюту, переводит национальную валюту на номер карты, указанный в заявке. Посредником выступает централизованная биржа. В момент принятия заявки криптовалюта продавца замораживается на эскроу-счете биржи, где ни одна из сторон сделки не имеет к ней доступа. Далее покупатель криптовалюты переводит денежные средства по указанным реквизитам и сигнализирует об осуществлении оплаты. Продавец проверяет, поступили ли денежные средства на счет, после чего подтверждает факт поступления денежных средств. Далее биржа размораживает криптовалюту и переводит ее покупателю.

В процессе вышеуказанного обмена злоумышленник, желающий похитить криптовалюту, совершает действия, направленные на то, чтобы продавец подтвердил факт получения денежных средств. Для этого он может направить SMS-сообщение на номер телефона продавца, которое будет идентично сообщению, которое обычно получают пользователи при зачислении денежных средств на банковский счет. Продавец, который должным образом не убедился в получении денежных средств, подтверждает факт их получения. В результате злоумышленник совершает хищение криптовалюты. Также злоумышленник может осуществить перевод меньшей

[27] РБК : сайт. URL: https://www.rbc.ru/crypto/news/682f0c1f9a79474bf2e0eecd?ysclid=mg7igyfad9463994643 (дата обращения: 27.08.2025).

суммы, чем указано в заявке. В обоих примерах злоумышленники рассчитывают на невнимательность пользователей.

Все то же самое может быть совершено за пределами peer-to-peer сервиса. Например, при взаимодействии с криптовалютным обменником или третьими лицами. Единственное отличие в том, что криптовалюта нигде не замораживается и подтверждения получения денежных средств не требуется. Подобные случаи нашли свое отражение в судебной практике.[28]

Существуют также способы хищения, рассчитанные на опытных пользователей. Так, например, злоумышленник намеренно предоставляет неограниченному кругу лиц, группе лиц или конкретному лицу данные для доступа к своему некастодиальному кошельку, на балансе которого имеется криптовалюта. Злоумышленник может сделать вид, что это произошло случайно, либо, якобы, попросить о помощи в совершении какого-либо действия (например, совершить транзакцию) за вознаграждение. Однако, как мы знаем, для совершения транзакции необходимо оплатить комиссию блокчейна, в котором находится эта криптовалюта. Как мы знаем, оплата производится в основной монете блокчейна. Так, например, если необходимо совершить транзакцию в сети «Ethereum», оплата должна быт произведена в ETH на блокчейне «Ethereum», если в сети «Binance Smart Chain», то в BNB на блокчейне «Binance Smart Chain» и т.д. Поэтому для совершения транзакции, для начала, необходимо пополнить баланс в основной монете блокчейна. Кошелек заранее подключен к программному обеспечению, функция которого заключается в автоматическом выводе из кошелька криптовалюты, в которой предполагается оплата комиссии. В результате, пополняемый баланс всегда обнуляется. Часто данный способ хищения рассчитан на неопределенный круг лиц. Поэтому мнемоническая фраза может быть размещена в чате

[28] См. например: приговор Октябрьского районного суда города Тамбова от 15.02.2019 № 1-134/19, приговор Дорогомиловского районного суда города Москвы от 20.06.2023 по делу № 1-85/2023, приговор Дорогомиловского районного суда города Москвы от 25.12.2024 № 01-0276/2024 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 01.07.2025).

мессенджера, в комментариях под размещенным контентом и т.д. Следует иметь ввиду, что в таких случаях сами потерпевшие могли совершить покушение на хищение, что может подтвердиться при осмотре истории транзакций кошелька, к которому дан доступ, а также соответствующего блокчейн обозревателя.[29]

Еще одним из таких способов является предпродажа или продажа токенов, которые заведомо для злоумышленников не несут и не будут нести никакой ценности. Для реализации преступного умысла злоумышленники создают либо покупают каналы в мессенджерах и аккаунты в различных социальных сетях, набирают «мертвую» аудиторию, чтобы создать иллюзию популярности. Далее канал оформляется как экспертный блог по заработку на криптовалюте, в нем регулярно публикуется полезная информация. Данный источник информации активно рекламируется злоумышленником для привлечения настоящих подписчиков. Полезный контент вызывает у подписчиков доверие. Далее злоумышленник начинает вводить свою аудиторию в заблуждение относительно технологической пользы проекта или проектов, которые он начал рекламировать, а также относительно событий, которые происходят в криптовалютной индустрии, чтобы аргументировать свои прогнозы относительно роста цен токенов и получения большой прибыли инвесторами.

Вышеуказанный способ легко вызывает доверие у многих пользователей, потому что действительно в 2013, 2017 и 2021 годах наблюдался экспоненциальный рост стоимости большого количества криптовалют. Злоумышленники также используют эти правдивые факты для аргументации своих прогнозов.

По этой причине, желая быстро и легко обогатиться, многие совершают покупку рекламируемых токенов за криптовалюту, которая имеет реальную

[29] Гайсин Н.И. Характеристика способов совершения хищений криптовалютных активов // Сибирские уголовно-процессуальные и криминалистические чтения. 2025. № 3. С. 36.

ценность.

Токен размещается на децентрализованной бирже в паре с криптовалютой, имеющей реальную ценность. То есть злоумышленник создает один или несколько пулов ликвидности, который состоит из криптовалюты, за которую он хотел бы продать рекламируемый токен, и рекламируемого токена (например, пул ликвидности BNB/X, где BNB является криптовалютой, имеющей реальную ценность, в обмен на которую возможности приобрести токен X, а X является рекламируемым токеном, не имеющим реальную ценность). Далее злоумышленник выкладывает на своем канале подробную пошаговую инструкцию о том, как купить данный токен, указывая идентификатор (контракт) токена, который необходимо указать в строке выбора покупаемого токена. Некоторые такие токены, действительно, показывают многократный рост для убедительности. Злоумышленник искусственно управляет ценой токена, чтобы завлечь как можно больше средств пользователей. Однако после покупки токена его невозможно продать. Злоумышленник ограничивает продажу токена через функции смарт-контракта. Он программирует смарт-контракт таким образом, что для продажи токена необходимо оплатить комиссию в размере 100 % стоимости суммы продажи.

Анализ судебной практики позволил выявить судебные акты по уголовным делам о мошенническом хищении криптовалют, где преступники обещали потерпевшим высокий уровень заработка или вводили в заблуждение, а также злоупотребляли доверием относительно иных обстоятельств.[30]

Большинство способов требуют подготовительных действий. Подготовка к совершению хищений криптовалютных активов может быть

[30] См. например: апелляционное определение Московского городского суда от 03.02.2025 по делу № 10-1253/2025, апелляционное определение Московского областного суда от 16.09.2025 по делу № 22-8217/2025, приговор Зеленоградского районного суда города Москвы от 24.05.2022 по делу № 1-93/2022 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 01.07.2025).

выражена в различных действиях или совокупности действий. В частности, в обучении работе с криптовалютой, созданию вредоносных программных обеспечений, смарт-контрактов и децентрализованных приложений, фишинговых сайтов и т.д.; приобретении устройств, с помощью которых возможно создать вредоносные программные обеспечения, смарт-контракты и децентрализованные приложения, фишинговые сайты и прочее; приобретении вредоносных программных обеспечений, а также в выборе способа анонимизирования личности преступника.

Соответственно, в этом случае, злоумышленник будет хранить на своих электронных носителях информации различные обучающие материалы по созданию вредоносных программ, фишинговых сайтов, схемам хищения криптовалюты, вредоносные программные коды и т.д., либо будет иметь онлайн доступ ко всему указанному через мессенджеры или сайты, о чем может свидетельствовать браузерная история посещений. Кроме того, в истории браузера может содержаться информация о посещении соответствующих форумов, маркет-плейсов и других Интернет-ресурсов.

Для сокрытия данных о личности преступника, могут быть приняты следующие меры:

– использование данных подставных лиц для прохождения процедуры верификации на криптовалютной бирже;

– оформление банковских карт на имя подставных лиц;

– использование VPN сервисов и прокси для сокрытия IP-адреса;

– использование анонимных блокчейнов, т.е. не отображающих адреса криптовалютных кошельков и другие данные в транзакциях блокчейн-обозревателей (Monero, Zcash, Dash и т.д.);

– уничтожение электронных следов (очищение истории посещений в браузере, удаление программного обеспечения, фишинговых сайтов, переписок и т.д.).

Таким образом, любой способ хищения направлен на:

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

2) Перевод криптовалюты самим потерпевшим в адрес злоумышленника;

3) Получение разрешения вредоносному децентрализованному приложению распоряжаться криптовалютой.

Нами были перечислены не все имеющиеся из возможных способов, поскольку с развитием компьютерных технологий, а также блокчейн технологий происходит появление новых и развитие ранее существовавших способов хищения криптовалютных активов, а также способов сокрытия данных об их хищении. Однако выше были раскрыты одни из наиболее актуальных и распространенных.

1.4. Иные элементы криминалистической характеристики хищения криптовалютных активов

Накопление и систематизация знаний о криминалистической характеристике хищений криптовалюты имеет практическое значение для органов предварительного расследования, поскольку эти знания могут помочь избрать наиболее подходящие организационные меры, выдвинуть следственные версии, а также выбрать верное направление первоначального этапа расследования.

Важным элементом криминалистической характеристики являются ***электронные (цифровые) следы***, неизбежно оставляемые в блокчейнах, на устройствах потерпевших и преступников, на серверах, а также в банковских базах данных. В блокчейнах остается информация о совершенных транзакциях, что позволяет отследить, на какой публичный адрес поступила криптовалюта от потерпевшего к преступнику. На устройствах потерпевших и преступников остаются различные 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 и многое другое. Отдельно следует отметить невидимые цифровые следы, которыми являются различные статистические данные о посещениях интернет-ресурсов, открытии файлов и программных обеспечений, история поисковых запросов, данные о местонахождении и передвижении устройства, его IP-адрес и т.д. Результативный поиск таких следов позволяет подтвердить связь с событием преступления и благодаря обнаруженным следам признать в дальнейшем осмотренные объекты вещественными доказательствами. Технически грамотный и тщательный осмотр отдельных предметов иногда ведет к обнаружению новых, ранее неизвестных доказательств.[31] Некоторые такие следы могут быть обнаружены только путем получения необходимой информации от владельцев серверов, обслуживающих интернет-ресурсы, которые посещали потерпевший и (или) преступник. Также следует пояснить, как могут помочь расследованию преступлений данные, предоставляемые банками. Поскольку криптовалюта имеет ценность, существуют лица, которые готовы обменять криптовалюту на национальную валюту и наоборот. Часто такие действия осуществляются путем банковского перевода на счет, который находится во владении преступника. При наличии информации о принадлежности криптовалютного кошелька (публичного адреса) конкретному лицу, которое совершило обмен для злоумышленника, имеются шансы на установление личности злоумышленника. Установить принадлежность криптовалютного кошелька конкретному лицу, которое совершило обмен для злоумышленника, возможно путем взаимодействия с органами, осуществляющими оперативно-розыскные мероприятия. Более подробно об осмотре и изъятии возможных цифровых следов нами будет рассмотрено в третьей главе диссертации.

[31] Макаренко И.А., Эксархопуло А.А. Сущность и правовые формы поисковой деятельности следователя // Философия права. 2024. № 4 (111). С. 149.

Следующий немаловажный элемент криминалистической характеристики – ***личность преступника***, совершившего хищение криптовалюты. Большинство хищений совершается лицами мужского пола в молодом возрасте. Предположение о молодом возрасте связано с недавним возникновением и развитием криптовалютной индустрии. Более молодые лица имеют больше свободного времени, а также более высокий потенциал к обучению работе с криптовалютой, поскольку легко взаимодействуют с персональным компьютером. Лица старшего возраста, в большинстве случаев, испытывают трудности при взаимодействии с персональным компьютером.

Ключевое значение имеет уровень профессиональной подготовки, наличие профильного образования, а также комплекса различных навыков, знаний и опыта (например, знания о существовании тех или иных программных обеспечений, предназначенных для взаимодействия с криптовалютой; создание вредоносных программных обеспечений; убедительность и т.д.). В зависимости от вида совершаемых хищений, преступник обладает той или иной совокупностью вышеперечисленного. Однако все преступники, непосредственно совершающие хищение криптовалют, имеют базовые навыки владения персональным компьютером, смартфоном, а также взаимодействия с криптовалютой.

Злоумышленники, специализирующиеся на тайных хищениях (без взаимодействия с потерпевшим), в подавляющем большинстве случаев имеют навыки и опыт в области программирования, создания вредоносных программ (или) децентрализованных приложений, фишинговых сайтов, а также способны обеспечить собственную анонимность в сети Интернет. Всему этому они могут обучиться как самостоятельно, так и в результате приобретения соответствующих курсов. Также они могут иметь образование в области информационных технологий. Некоторые из них обладают хорошими коммуникативными навыками, убедительны при ведении письменных или устных диалогов (как правило, такими навыками обладают пособники, если

преступление совершается группой лиц по предварительному сговору).[32] В подтверждение вышеуказанного существует судебная практика, где хищение совершено лицом, обладающим специальными знаниями в сфере компьютерной информации, которое намеренно устроилось на работу в организацию, являвшуюся собственником криптовалюты. В силу своих обязанностей преступник получил необходимые доступы к исходным кодам и, воспользовавшись своими навыками, похитил приватный ключ от криптовалютного кошелька.[33]

Специальные навыки не требуются в тех случаях, когда тайные хищения совершаются лицами, получившими доступ к устройству собственника криптовалюты и всем необходимым программным обеспечениям, содержащимся в этом устройстве, либо к мнемонической фразе или приватному ключу собственника. В таких случаях достаточно базовых навыков владения персональным компьютером, смартфоном, а также навыков работы с программным обеспечением, предназначенным для работы с криптовалютой. В судебной практике имеется случай, когда преступник получил доступ к кошельку ввиду наличия возможности тайно завладеть устройством, на котором было установлено приложение, предоставляющее доступ к криптовалюте.[34]

Злоумышленникам, специализирующимся на хищениях путем обмана или злоупотребления доверием, помимо базовых навыков, достаточно обладать хорошими коммуникативными навыками и навыками убеждения. Если они обладают знаниями, необходимыми для совершения тайных хищений (например, создание вредоносных смарт-контрактов и

---

[32] Гайсин Н.И. К вопросу об элементах криминалистической характеристики хищения криптовалютных активов // Философия права. 2025. № 2. С. 116.

[33] Приговор Дорогомиловского районного суда города Москвы от 27.11.2023 по делу № 1-645/2023 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 14.06.2025).

[34] Приговор Октябрьского районного суда города Ижевска от 26.11.2024 по делу № 1-318/2024 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 14.06.2025).

децентрализованных приложений), то они способны реализовывать более сложные схемы по хищению криптовалют. Для злоумышленников, реализующих сложные схемы хищений, характерно тщательное планирование, подготовка к будущим хищениям и сокрытие следов их совершения.

Некоторые из таких преступников могут иметь опыт совершения хищений безналичных денежных средств, а также судимости по соответствующим статьям УК РФ в прошлом.

Интересным является систематизация знаний о характерных чертах личности типичных преступников в зависимости от уровня соответствующих познаний, представленная Е.А. Хариной:

1. Специалисты высокого уровня, обладающие незаурядными познаниями, часто являются разработчиками высококвалифицированных компьютерных программ. К выбору объекта преступного воздействия относятся избирательно, с азартом проявляя интерес к труднодосягаемым целям;

2. Преступники, обладающие большим опытом в сфере компьютерных технологий. Имеющийся уровень познаний не позволяет таким преступникам являться разработчиками компьютерных программ, при этом, помимо активного использования, могут заниматься их модернизацией. Выбору объекта преступного посягательства особого значения не придают;

3. Специалисты среднего уровня, обладающие соответствующими познаниями на уровне уверенных пользователей. Подобная деятельность у таких специалистов характеризуется устойчивой увлеченностью, особенностью уровня развития сознания является фрагментарное видение ситуации;

4. Специалисты, обладающие невысоким, обывательским уровнем познаний в сфере компьютерной информации. Преступную деятельность могут начать с совершения преступлений, не требующих особых познаний. Обладают высокой степенью неуверенности и настороженности, при этом в

общении с окружающими могут присутствовать амбициозность, эмоциональность, хвастовство.[35]

Несмотря на то, что такая классификация разработана для характеристики личности мошенников в сфере компьютерной информации, на наш взгляд, она хорошо подходит для систематизации знаний о криминалистической характеристике лиц, совершающих хищение криптовалюты.

Многие из рассматриваемых преступников официально не трудоустроены и не имеют стабильного источника дохода. Злоумышленники, реализующие сложные схемы хищений, в прошлом могли иметь опыт работы в сфере, связанной с информационными технологиями.

В зависимости от характера связи с потерпевшим могут быть выделены посторонние лица, случайные знакомые, а также близкие знакомые или родственники. В большинстве случаев преступники являются посторонними по отношению к потерпевшим, так как подавляющее большинство хищений является результатом беспечности и несоблюдения мер безопасности самими потерпевшими. Для того, чтобы прийти к выводу о том, что преступление, вероятнее всего, совершено знакомым или близким, необходимо провести ряд следственных действий. В частности, необходимо исключить факты: наличия вредоносных программ на устройстве, где установлены приложения, предоставляющие доступ к криптовалюте; добровольной передачи мнемонической фразы или приватного ключа посторонним; добровольного перевода похищенной криптовалюты постороннему лицу, а также одобрения самим собственником вредоносным децентрализованным приложениям распоряжаться криптовалютой. Исключение этих фактов посредством производства осмотров позволит сделать вероятностный вывод о том, что

[35] Харина Е.А. К вопросу о криминалистической характеристике мошенничества в сфере компьютерной информации // Российский следователь. 2023. № 11. С. 11-15. [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 14.06.2025).

хищение могло быть совершено знакомым потерпевшему лицом.

Аналогично и остальные электронные (цифровые) следы в виде переписок, различных файлов (фотографии, видеозаписи, аудиозаписи и т.д.), программных обеспечений, статистических данных о посещениях интернет-ресурсов, открытии файлов и программных обеспечений, истории поисковых запросов и т.д. представляют вероятностный вывод о личности преступника.

Еще один важный элемент криминалистической характеристики – ***личность потерпевшего***. Большинство потерпевших, на наш взгляд, также, как и преступники, находятся в молодом возрасте. Причины молодого возраста также связаны с относительно недавним появлением криптовалюты. Поскольку криптовалюта появилась относительно недавно, то и потерпевшие от её хищения относятся к молодому поколению, которое более приспособлено к взаимодействию с криптовалютой. Следует также добавить, что именно более молодое поколение имеет повышенный интерес к информационным технологиям.

У большинства потерпевших отсутствует образование в сфере информационных технологий и (или) углубленные знания в данной сфере, что делает их более уязвимыми перед злоумышленниками. Выражаться это может как в беспечном отношении к информационной безопасности в целом (например, отсутствие установленных антивирусных программ и других средств защиты, скачивание вирусных программ, использование сомнительных Интернет-ресурсов), так и в легкомысленном отношении к безопасности при взаимодействии с криптовалютой (хранение входных данных от биржевых аккаунтов и криптовалютных кошельков на том же устройстве, с помощью которого происходит взаимодействие с криптовалютой, либо в онлайн среде; подключение кошельков к непроверенным децентрализованным приложениям; бесконтрольное и часто бессознательное предоставление разрешений на использование имеющейся криптовалюты; необдуманное совершение сделок, а также невнимательность при совершении транзакций).

То же самое следует отметить и про финансовую грамотность. Отсутствие у потерпевших базовых знаний о финансовой грамотности позволяет легче ввести потерпевших в заблуждение относительно возможного заработка, а также приводит их к совершению необдуманных действий, из-за которых они теряют свою криптовалюту в результате хищения. В частности, действия могут быть направлены на получение быстрого заработка.

При этом для многих потерпевших характерно прохождение различных курсов по взаимодействию с криптовалютой. Однако это обучение является сегментарным, не имеет практической апробированности и не контролируется соответствующими специалистами, что не позволяет охватить всю необходимую базу знаний в отношении функционирования криптовалют и сделок с ними.[36]

Отдельно следует охарактеризовать поведение потерпевших в киберпространстве и их личностные качества. Поведение характеризуется активностью и целенаправленностью использования различных интернет-ресурсов и их инструментов. Анализ такой активности способен показать, какие сайты и площадки посещает пользователь, какие действия с криптовалютами совершает, с какими иными пользователями взаимодействует, а также каков характер такого взаимодействия. Для молодых пользователей характерна чрезмерная демонстративность своей жизни и достатка в социальных сетях, что является провоцирующим фактором для совершения в отношении них хищений. К личностным качествам потерпевших по делам о хищениях в сфере оборота криптовалют можно отнести невнимательность и беспечность, которыми активно пользуются «фишеры», хакеры и вымогатели, доверчивость и желание быстрого заработка, на которые делают упор злоумышленники, самоуверенность в том, что они никогда не станут жертвами киберпреступников, поскольку их

[36] Шнейдерова Д.И. Особенности криминалистической характеристики личности потерпевшего по делам о хищениях в сфере оборота криптовалют // Актуальные вопросы права, образования и психологии. 2021. Т 9. С. 151.

криптовалютное состояние не столь велико, чтобы привлечь чье-то внимание.[37]

[37] Шнейдерова Д.И. Указ. соч. 2021. Т 9. С. 152.

Глава 2. Организационные особенности первоначального этапа расследования дистанционных хищений криптовалютных активов

2.1. Основания возбуждения уголовного дела о хищении криптовалютных активов, содержание этой стадии расследования

Первоначальный этап расследования хищений криптовалютных активов характеризуется открытостью информации об объективных признаках совершенного преступления (информация о времени, размере и, нередко, способе хищения лежит на поверхности) и дефицитом информации о лице, совершившем хищение. В этой связи задачей расследования является закрепление криминалистически значимой информации об объективных признаках преступления, а на основании установленных обстоятельств и фактов, поиск и закрепление криминалистически значимой информации о лицах, причастных к хищению.

На данном этапе расследования хищения криптовалютных активов существует ряд организационных особенностей, знание которых поможет выдвинуть типичные следственные версии, собрать необходимые доказательства, уточнить выдвинутые версии на основании собранных доказательств и проверить их.

Ключевая роль принадлежит руководителю следственного органа и (или) начальнику органа дознания, основной функцией которых является организация деятельности по выявлению и раскрытию преступлений этого вида. От того, насколько быстро следователем (дознавателем) будут проведены неотложные следственные действия по уголовному делу, зависит эффективность обнаружения и изъятия доказательств по данной категории дел. Существующая практика показывает, что при расследовании преступлений, совершенных с использованием криптовалюты, руководитель должен четко представлять, кто из сотрудников обладает достаточной квалификацией и опытом работы по выявлению и раскрытию такой категории преступлений,

поскольку здесь требуются дополнительные знания из области экономики и финансов, компьютерных технологий и защиты информации.[38]

Первоначальный этап расследования хищений криптовалюты начинается со стадии возбуждения уголовного дела. Поскольку криптопреступления сравнительно недавно вошли в «преступный оборот», правоприменительная деятельность все чаще сталкивается с различными проблемами на стадии возбуждения уголовного дела, а доктринальные источники, как правило, не содержат решений для их преодоления.[39]

Некоторые авторы научных работ выделяют особое место подготовке к проверке сообщений о криптопреступлениях. Так, например, А.А. Титов аргументирует это тем, что:

1. Совершение преступлений с использованием криптовалюты сопровождается технологической спецификой;

2. Совершаемые операции носят децентрализованный характер, т.е. оборот криптовалюты происходит без определенного административного центра (в отличие от банковской системы), контролирующего операционные процессы;

3. Действия криптовладельца анонимны – блокчейн-технология связывает в цепочки всех пользователей, в результате чего нужный цифровой след законспирирован.[40]

Поэтому для эффективной проверки сообщения о преступлении следователю (дознавателю) необходимо знание, как минимум, понятийного аппарата о взаимодействии с криптовалютой. Отсутствие таких знаний не позволит произвести проверку надлежащим образом и может привести к

[38] Ишин И.А. Особенности производства отдельных следственных действий и роль начальника органа дознания при расследовании преступлений, совершенных с использованием криптовалют // Сетевое издание «Академическая мысль». 2020. № 2 (11). С. 84.

[39] Титов А.А. Отдельные особенности рассмотрения сообщений (заявлений) о преступлениях, совершенных с использованием криптовалют // Вестник Академии Следственного комитета Российской Федерации. 2023. № 2(36). С. 123.

[40] Титов А.А. Указ. соч. 2023. С. 123.

ошибочному решению.

Помимо проблем, стадии возбуждения уголовных дел по фактам хищений криптовалюты присущи некоторые особенности. Например, последовательность, совокупность и содержание следственных действий не похожа на последовательность, совокупность и содержание следственных действий, которые обычно производят при совершении хищений других объектов гражданского права, в том числе и безналичных денежных средств. Чаще всего, на данной стадии не только ничего неизвестно о лице, совершившем хищение, но и заявитель мог вовсе не взаимодействовать с таким лицом даже по переписке в сети Интернет. Например, если по собственной неосмотрительности осуществил ввод мнемонической фразы от своего криптовалютного кошелька в фишинговом браузерном расширении, выдающем себя за криптовалютный кошелек.

Первоочередное производство осмотра места происшествия, а также предметов и электронных устройств без получения подробных пояснений от заявителя, как правило, нецелесообразно, поскольку у следователя (дознавателя) еще нет информации как об объектах, подлежащих осмотру, так и о том, какая именно информация подлежит осмотру. По этой причине целесообразно, в первую очередь, получить подробное объяснение от заявителя, а далее произвести осмотры и другие следственные действия и оперативно-розыскные мероприятия на основании полученной информации.

Верно отметила Д.И. Шнейдерова, что для хищений в сфере оборота криптовалют характерен устоявшийся комплекс первичных мероприятий, который включает получение объяснений от заявителя (потерпевшего), проведение осмотров, направление запросов. Объяснения – отправная точка проверки и в то же время ключевой источник информации о совершенном преступлении. Из содержания объяснений устанавливается предмет преступного посягательства, общие сведения о способе хищения и задействованных при этом технических и программных средствах, характер и объем наступивших последствий. Кроме того, данные, полученные от

заявителя, позволяют наметить объекты последующих осмотров, а также сведения, которые требуют проверки и подтверждения посредством направления различным организациям запросов.[41]

Объектами осмотра обязательно должны быть электронные носители информации, с которых имеется доступ к криптовалюте а также, непосредственно, криптовалютные кошельки (биржевые аккаунты) и блокчейн-обозреватели.

Если заявитель и злоумышленник использовали только некастодиальные кошельки, невозможно запросить какую-либо информацию у третьих лиц, как, например, у банков или криптовалютных бирж, поскольку они не располагают необходимой информацией, что является как особенностью, так и проблемой.

Однако основной проблемой данной стадии, на наш взгляд, является определение достаточности оснований для принятия решения о возбуждении уголовного дела, поскольку затруднительно установить факт принадлежности криптовалюты заявителю, непонятно, как определить размер причиненного ущерба от хищения и какой совокупностью доказательств подтверждается наличие факта хищения.

Таким образом, в целях установления обстоятельств и фактов, указывающих на наличие признаков хищения, обязательными мероприятиями являются получение объяснений от заявителя и осмотр устройств, через которые имеется доступ к криптовалюте. Именно осмотр позволит установить наличие транзакции, в результате совершения которой произошло хищение, а также наличие иных сведений, имеющих значение для дела.

Достаточность оснований для возбуждения уголовного дела при разных способах совершения хищения определяется по-разному. На наш взгляд, в

[41] Шнейдерова Д.И. Типичные следственные ситуации по материалам проверки и уголовным делам о хищениях в сфере оборота криптовалют // Концептуальные основы современный криминалистики: теория и практика: материалы научно-практической конференции с международным участием, посвященной 50-летию со дня образования кафедры криминалистики юридического факультета Белорусского государственного университета. Минск, 13 апреля 2023 г. С. 343.

любом случае существует несколько обязательных данных, указывающих на признаки преступления, и ряд дополнительных данных, необходимость в которых определяется в зависимости от результатов действий следователя (дознавателя), направленных на проверку наличия обязательных оснований. Обязательным для возбуждения уголовного дела является наличие:

1. Объяснения заявителя, в котором он утверждает, что транзакция совершена им под влиянием обмана или злоупотребления доверием, либо совершена не им и в результате причинен ущерб в размере эквивалентном более 2500 рублей (в случаях, когда имеются явные признаки совершения хищения группой лиц, размер похищенного не имеет значения);

2. Протокола осмотра электронного носителя информации, с которого имеется доступ к криптовалюте, а именно, криптовалютного кошелька заявителя и блокчейн-обозревателя, в котором:

А) зафиксирован публичный адрес заявителя, с которого совершена транзакция;

Б) зафиксирован факт наличия транзакции или транзакций, в результате совершения которых заявителю причинен ущерб в размере, эквивалентном более 2500 рублей, если отсутствуют признаки хищения группой лиц.

Под транзакциями, в результате совершения которых заявителю причинен ущерб, следует понимать не только транзакцию по осуществлению перевода криптовалюты с одного публичного адреса на другой, но и другие транзакции (например, по предоставлению разрешения децентрализованному приложению распоряжаться криптовалютой).

Кроме того, необходимы подтверждения того, что средства на кошельке принадлежат заявителю, как, например, объяснения очевидцев, протоколы осмотров электронных носителей информации, с которых 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 и т.д.

Размер причиненного ущерба, как правило, подтверждается заключением эксперта и на стадии предварительного расследования такое заключение необходимо. На стадии проверки сообщения о преступлении, на наш взгляд, обязательность наличия такого заключения зависит от того, какая криптовалюта похищена и в каком количестве. Если похищена известная широкому кругу лиц криптовалюта, как BTC, ETH, USDT, USDC или любая другая криптовалюта, прошедшая процедуру размещения на одной или нескольких криптовалютных биржах, определить размер похищенных средств не составит труда, поскольку информация о стоимости криптовалюты имеется в открытых источниках. В таких случаях очевидно, что размеры похищенного образуют состав соответствующей статьи УК РФ. На этапе возбуждения уголовного дела полагаем, что будет достаточно протокола осмотра электронного носителя информации, а именно, онлайн источника, который позволяет установить стоимость конкретной криптовалюты в конкретное время и дату. Таким источником, к примеру, может быть сайт в сети Интернет с URL-адресом https://ru.tradingview.com, позволяющий просмотреть курс отдельно взятой криптовалюты к доллару США на популярных криптовалютных биржах в отдельно взятый отрезок времени, вплоть до одной секунды. Полученный результат следует умножить на официальный курс доллара США, установленный ЦБ РФ. Такой подход видится более эффективным, с точки зрения экономии времени и ресурсов. Однако при наличии сомнений или появления затруднений, стоит проконсультироваться со специалистом или назначить экономическую экспертизу для определения стоимости похищенного. Это особенно актуально, когда нет уверенности в том, что рублевый эквивалент похищенной криптовалюты равен или больше минимальной суммы, хищение которой образует состав преступления, а признаки хищения группой лиц отсутствуют. В этом случае экспертное заключение экономиста необходимо для определения точной суммы хищения и принятия решения на стадии возбуждения уголовного дела. Дело в том, что стоимость криптовалюты определяется рыночными условиями и в одно и то

же время цены на разных площадках могут в незначительной степени отличаться друг от друга. Также необходимо принять во внимание, если злоумышленник совершил транзакцию с кошелька заявителя, он потратил часть средств на уплату комиссий, чтобы совершить хищение, что также должно быть учтено в сумме похищенного. Необходимо точно определить, образует ли совершенное хищение состав преступления или административного правонарушения.

Следует отметить, что могут быть ситуации, когда похищена криптовалюта, не прошедшая процедуру размещения на централизованных криптовалютных биржах, в том числе и NFT, что может усложнить определение ее точной стоимости на момент хищения, а также может поставить под сомнение ее ценность. В подобных ситуациях считаем, что обязательно наличие заключения экономиста. Некоторые новые или непопулярные криптовалюты могут быть не размещены на централизованных биржах и их купля-продажа возможна только посредством децентрализованных бирж или NFT маркетплейсов, что может затруднять определение стоимости, особенно, для неопытных пользователей криптовалютной индустрии. Учитывая, что в подобной ситуации могут понадобиться знания в области взаимодействия с децентрализованными приложениями, необходимо привлечь специалистов, которые проконсультируют относительно постановки вопросов при назначении экономической, компьютерно-технической и других экспертиз.

В зависимости от содержания объяснений заявителя и результатов осмотров, необходимо установить ряд других обстоятельств и фактов, которые будут являться основанием для возбуждения уголовного дела.

Если заявитель в своем объяснении сообщил о том, что хранил свою криптовалюту на кастодиальном кошельке (биржевом аккаунте) и лично не осуществлял ее перевод в адрес злоумышленников, для возбуждения дела необходим протокол осмотра, согласно которому в истории посещений криптовалютного кошелька имеется IP-адрес иного интернет-провайдера,

который ранее не выделялся для собственника криптовалюты, владеющего биржевым аккаунтом, а также сведения об устройстве, применявшемся для посещения биржевого аккаунта, которое ранее не использовалось владельцем. В отсутствие такой информации, в истории посещений должны быть сведения о времени посещения, в которое владелец лично не осуществлял вход в биржевой аккаунт. Вышеуказанную информацию также возможно запросить у криптовалютной биржи.

Если криптовалюта хранилась на некастодиальном кошельке и заявитель лично не осуществлял перевод криптовалюты в адрес злоумышленников, а также не предоставлял разрешений децентрализованным приложениям распоряжаться криптовалютой, необходимы протоколы осмотров электронных носителей информации заявителя, в которых зафиксированы факты передачи третьим лицам данных, позволяющих получить доступ к криптовалюте. При отсутствии таких доказательств, необходимо заключение компьютерно-технической экспертизы, в котором указано, что на устройствах заявителя имеется вредоносное программное обеспечение с функциями, позволяющими похитить криптовалюту, либо способствующими такому хищению.

Если заявитель незадолго до хищения взаимодействовал с третьими лицами и выполнял их просьбы или следовал их инструкциям, следует осмотреть переписки с ними, принять меры к восстановлению переписок, если они удалены, после чего получить доказательства того, что заявитель выполнил их просьбу или последовал их инструкции. Такие просьбы и инструкции могут заключаться в передаче данных для получения доступа к криптовалюте, переводу криптовалюты на указанный адрес, переходу по обозначенным URL-адресам и выполнении ряда действий на указанных URL-адресах, загрузке файлов и т.д. Выполнение просьб или инструкций может подтверждаться осмотрами блокчейн-обозревателей, истории посещений веб-страниц с помощью интернет-браузеров и другой компьютерной информацией.

В случаях, когда заявитель по каким-то причинам потерял доступ к биржевому аккаунту и не может восстановить его, что препятствует производству необходимых осмотров, достаточным основанием для возбуждения уголовного дела будут являться объяснение заявителя, а также протоколы осмотров электронных носителей информации заявителя в той части, где видно, что произошло списание средств; незадолго до хищения у заявителя был доступ к кошельку; онлайн-источника, подтверждающего достаточность размера хищения для возбуждения уголовного дела; а также блокчейн-обозревателя. О списании средств может свидетельствовать, например, уведомление из электронной почты, прикрепленной к биржевому аккаунту. В данном уведомлении можно увидеть ID транзакции, а также взаимодействовавшие публичные адреса (адрес заявителя и адрес злоумышленника). О наличии доступа к биржевому аккаунту ранее могут свидетельствовать уведомления и электронные письма, из которых видно, что пользователь взаимодействовал с биржевым аккаунтом. Это могут быть сохраненные ранее уведомления о зачислениях или выводе средств, а также совершении каких-либо сделок внутри биржи. В сложившейся ситуации необходимо принять все возможные меры к восстановлению доступа к биржевому аккаунту. По сравнению с некастодиальным кошельком, пользователю не нужно сохранять приватные ключи и мнемоническую фразу. Достаточно принять меры к смене пароля от личного кабинета (биржевого аккаунта).

Если у заявителя нет доступа к некастодиальному кошельку, восстановление утерянного доступа к кошельку без мнемонической фразы или приватного ключа невозможно. В данной ситуации подтвердить факт хищения возможно только при наличии информации об ID транзакции и (или) публичных адресах (адреса заявителя и адреса злоумышленника).

Поскольку обстоятельства хищения могут быть разными, невозможно перечислить все возможные варианты достаточных оснований для возбуждения уголовного дела.

Вместе с тем, выделены обязательные для принятия решения о возбуждении уголовного дела данные, указывающие на признаки преступления, которыми являются:

1. Объяснение заявителя, в котором он указывает на совершение хищения принадлежащей ему криптовалюты, стоимость которой эквивалентна сумме более 2500 рублей (при отсутствии явных признаков хищения группой лиц), с описанием всех имеющих значение обстоятельств и фактов;

2. Протоколы осмотров электронных носителей информации, а именно:

А) истории транзакций криптовалютного кошелька (биржевого аккаунта) и блокчейн-обозревателей, из которых видно транзакцию, в результате совершения которой произошло хищение;

Б) истории транзакций в банковских приложениях, переписок в мессенджерах, электронных писем, других цифровых следов и иных доказательств, свидетельствующих о покупке (принадлежности) криптовалюты заявителю;

В) онлайн источников информации о стоимости похищенной криптовалюты;

В зависимости от размера совершенного хищения, способа хранения криптовалюты, совершения транзакции самим заявителем или злоумышленником, дополнительными данными, указывающими на признаки преступления, являются:

1. Заключения экономической и (или) компьютерно-технической экспертиз, согласно которым стоимость похищенной криптовалюты свыше 2500 рублей (при отсутствии явных признаков хищения группой лиц) и (или) на электронных носителях информации, откуда имелся доступ к криптовалюте, имеется вредоносное программное обеспечение, обладающее функциями, позволяющими похитить криптовалюту, или способствующими ее хищению, соответственно;

2. Протоколы осмотров электронных носителей информации заявителя, а именно, истории посещений браузеров, переписок в социальных сетях, мессенджерах и других сервисах;

3. Ответы организаций на запросы следователя (дознавателя);

4. Объяснения очевидцев, прямо или косвенно подтверждающие факт хищения.

Вышеуказанный перечень не является закрытым.

В рамках возбужденного уголовного дела необходимо произвести осмотры остальных объектов, которые не были осмотрены на стадии возбуждения уголовного дела и назначить необходимые экспертизы (как правило, экономическую и компьютерно-техническую). Если по результатам осмотров есть основания полагать, что с кошельком злоумышленника взаимодействовали криптовалютные биржи и обменники, необходимо инициировать запросы в адрес криптовалютных бирж, а также организовать проведение обысков по местам нахождения обменников и других необходимых следственных действий (например, арест криптовалюты, хранящейся посредством некастодиального криптовалютного кошелька). К проведению осмотров, допросов и обысков следует привлекать специалистов. Такими специалистами могут быть блокчейн и веб-разработчики со знанием различных языков программирования, блокчейн-инженеры, криптоброкеры, майнеры, специалисты по обеспечению кибербезопасности, системные администраторы, криптографы и другие.[42]

Для получения информации о том, на чье имя зарегистрирован биржевой аккаунт, необходимо направить запрос в адрес соответствующей биржи. На сайтах крупных криптобирж, сотрудничающих с правоохранительными органами, есть специальный раздел, в котором идет речь о взаимодействии. Например, на сайте криптовалютной биржи «Binance» есть разделы «Руководство для правоохранительных органов» и «Система запросов для

[42] Шнейдерова Д.И. Использование специальных знаний при расследовании хищений в сфере оборота криптовалют // Вестник криминалистики. 2020. № 4(76). С. 105.

правоохранительных органов», где подробно расписан порядок взаимодействия. Так, например, запросы для правоохранителей из Российской Федерации можно направлять по адресу эл. почты (case@binanceholdings.ru). Мониторинг сайтов известных криптовалютных бирж, популярных в Российской Федерации, показал, что на их сайтах всегда указан электронный адрес для связи с правоохранительными органами.[43] К сожалению, никаких гарантий получения ответа на запрос от криптовалютной биржи нет. Часть опрошенных респондентов, в чьем производстве были уголовные дела о хищениях криптовалюты, и направившие запросы в адрес криптовалютных бирж, не получили ответы на свои запросы (Приложение 1).

2.2. Типичные следственные ситуации и версии при расследовании хищений криптовалютных активов

Не останавливаясь на теоретических основах таких категорий, как следственная ситуация и версия, которым посвятили свои работы Р.С. Белкин, Л.Я. Драпкин, Л.Л. Каневский, Т.С. Волчецкая, И.М. Комаров, И.Ф. Герасимов, В.К. Гавло [44] и др., присоединяемся к обобщенному выводу, к которому пришла В.Г. Бабанина в своей диссертации: «1) под следственной

[43] Хайдаров А.А. Установление владельца адреса криптокошелька в практике правоохранительных органов // Российский следователь. 2024. № 8. С. 39-42. [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 14.06.2025).

[44] См.: Белкин Р.С. Криминалистика: проблемы, тенденции, перспективы. – М.: Юрид. лит., 1988. – С. 91-92, Драпкин, Л.Я. Построение и проверка следственных версий: автореф. дис. … к-та юрид. наук. Москва, 1972. 28 с., Каневский Л.Л. Криминалистическая характеристика преступления, криминальные и следственные ситуации и их значение в раскрытии и расследовании преступлений несовершеннолетних // Вопросы совершенствования борьбы с преступностью несовершеннолетних. – Уфа: Изд-во БашГУ, 1983. – С. 79-80, Волчецкая Т.С. Криминалистическая ситуалогия: автореф. дис. ... д-ра юрид. наук. Москва, 1997. 48 с., Комаров И.М., Пономаренко Н.Ю., Ян Е.И. Ситуационный подход как научно-практическая категория криминалистики // Сибирские уголовно-процессуальные и криминалистические чтения. 2017. № 3 (17). С. 104-115, Герасимов И.Ф. К вопросу о следственной ситуации // Следственная ситуация: Сб. науч. тр. – М.: Всесоюз. ин-т по изучению причин и разработке мер предупреждения преступности, 1984. – С. 6, Гавло В.К. Следственная ситуация // Следственная ситуация: Сб. науч. тр. – С. 40.

ситуацией следует понимать совокупность конкретных обстоятельств, имеющихся на данный момент расследования; 2) изучение типовых следственных ситуаций конкретного вида (группы) преступлений является обязательным элементом при разработке криминалистических рекомендаций (частных методик) по эффективному расследованию преступлений на первоначальном этапе».[45]

На первоначальном этапе расследования дел о хищениях криптовалют можно выделить четыре варианта сложившихся следственных ситуаций:

1. Данные, указывающие на личность преступника, отсутствуют, он не установлен и не задержан;

2. Имеются данные, указывающие на личность преступника, но он не установлен и не задержан;

3. В деле имеются сведения, указывающие на личность преступника, он установлен, но не задержан;

4. Имеются сведения, указывающие на личность преступника, он установлен и задержан.[46]

Несмотря на прозрачность транзакций в блокчейне и возможность отследить движение всех средств, выдвинуть различные следственные версии, следственная ситуация на первоначальном этапе расследования редко может быть благоприятной, поскольку злоумышленникам не нужно вступать в контакт с лицами, у которых они похищают криптовалюту, либо такой контакт может ограничиваться переписками, для которых часто создаются отдельные учетные записи с использованием данных, не подлежащих идентификации, а также используются средства анонимизации. Более того, злоумышленники могут находиться на территории зарубежных стран, что в значительной степени осложняет расследование или делает его продолжение невозможным.

[45] Бабанина В.Г. Первоначальный этап расследования хищений в сфере дорожного строительства: диссер. … канд. юрид. наук. Краснодар, 2025. С. 103-104.

[46] Шнейдерова Д.И. Указ. соч. 2023. С. 347.

В большинстве случаев, на первоначальном этапе расследования следователь (дознаватель) может располагать сведениями о характере совершенного хищения, однако у него будут отсутствовать сведения о преступнике. Редко могут иметь место случаи, когда будет известно о лице, совершившем хищение. Такое возможно, если потерпевший сам сообщит о лице, которое совершило хищение или причастно к хищению, либо злоумышленник не предпринимал каких-либо попыток скрыть свою личность, использовал личные учетные записи мессенджеров или социальных сетей, а также оставил цифровые следы, по которым не составит труда установить его личность.

Что касается следственных версий, невозможно переоценить практическую значимость из типизации, состоящей в вычленении наиболее схожих черт различных ситуаций, формировании и выделении на этой основе наиболее характерных предположений о событии, образованных совокупностью аналогичных друг другу обстоятельств. Опираясь на результаты обобщения практики, выделяя в ней наиболее характерные закономерности, типичная версия позволяет следователю определенным образом построить его мышление в ходе работы по уголовному делу. То есть при использовании типичных версий конструирование мысленной модели события, производимого в ходе расследования, происходит с учетом готового решения, хоть и поверхностного, лишь задающего направление познавательной деятельности.[47]

Типизируя следственные версии, важно учитывать исходные данные, которые в свою очередь можно классифицировать по критериям полноты сведений о сущности события, субъекте, мотиве, а также обстоятельствах преступления.[48]

---

[47] См. например: Белкин Р.С., Винберг А.И., Дорохов В.Я. и др. Теория доказывания в советском уголовном праве. М.: Юрид. лит., 1973. С. 342., Баев О.Я. Основы криминалистики: курс лекций. М.: Экзамен, 2001. С. 24.

[48] Арцишевский Г.В. Выдвижение и проверка следственных версий. М.: Юрид. лит., 1978. С. 53.

В условиях дефицита информации о лице, совершившем хищение, в первую очередь, следует сосредоточиться на выдвижении версий об объективных признаках преступления. На основе этих версий следует выдвинуть и проверить версии о личности преступника.

Следует отметить, что выдвижение одних типичных версий в совокупности с имеющей значение для дела информацией позволяет выдвинуть более подробные версии.

Наиболее простым видится выдвижение типичной следственной версии о способе хищения (в результате использования входных данных; предоставления разрешения децентрализованному приложению распоряжаться криптовалютой; самостоятельного перевода криптовалюты в адрес злоумышленника), поскольку для выдвижения этой версии необходимо установить минимальную совокупность обстоятельств и фактов:

1. Способ хранения похищенной криптовалюты.
2. Инициатора транзакции.

Если похищенная криптовалюта хранилась на кастодиальном кошельке (биржевом аккаунте), версия о хищении в результате предоставления разрешения децентрализованному приложению распоряжаться криптовалютой теряет свою актуальность.

Если инициатором транзакции является сам потерпевший, отпадает версия о хищении в результате использования злоумышленником входных данных.

После двух вышеуказанных обстоятельств, появляется возможность выдвинуть ряд более подробных следственных версий о способе хищения.

Если похищенная криптовалюта хранилась на кастодиальном кошельке (биржевом аккаунте) и при этом неправомерную транзакцию совершил злоумышленник, следует выдвинуть и проверить две следственные версии:

1. Хищение криптовалюты совершено в результате получения третьими лицами доступа к биржевому аккаунту заявителя (потерпевшего).

2. Хищение криптовалюты совершено в результате хакерской атаки на биржу.

Информация о совершении хакерской атаки на биржу достаточно быстро появляется в различных источниках средств массовой информации. Поэтому вторую версию целесообразно выдвигать в случае появления соответствующей информации во множествах информационных источников. В большинстве случаев, биржи имеют официальные страницы в социальной сети «Х» (запрещенная социальная сеть на территории Российской Федерации). Поэтому наиболее достоверным источником информации о хакерском взломе будет являться соответствующая информация на официальной странице социальной сети.

В отсутствие вышеуказанной информации следует выдвинуть и проверить первую версию.

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

1. Хищение криптовалюты совершено в результате обмана или злоупотребления доверием;

2. Факт хищения отсутствует ввиду добросовестного заблуждения заявителя.

Выдвижение более подробной версии о способе хищения зависит от обстоятельств, при которых злоупотребили доверием заявителя (потерпевшего) или относительно чего он был введен в заблуждение. Наиболее распространенными вариантами являются обман или злоупотребление доверием относительно возможности заработка, либо относительно приобретения товара или оказания услуги. Для введения в заблуждение относительно заработка, злоумышленники могут сообщить потерпевшему как о несуществующих, так и существующих схемах заработка, которые, якобы, возможно реализовать после перевода криптовалюты по указанному ими адресу. Это, может быть, как адрес кошелька, так и децентрализованное приложение, находящееся под контролем злоумышленника. Относительно

приобретения товаров или оказания услуг существует множество различных вариаций, перечисление которых нецелесообразно. Одним из самых распространенных является хищение на peer-to-peer платформах бирж, когда пользователи совершают обмен криптовалюты на национальную валюту.

Если похищенная криптовалюта хранилась на некастодиальном кошельке и транзакцию по переводу криптовалюты совершил злоумышленник, следует выдвинуть и проверить три следственные версии:

1. Хищение криптовалюты совершено в результате получения третьими лицами доступа к некастодиальному кошельку заявителя (потерпевшего);

2. Хищение криптовалюты совершено в результате предоставления разрешения вредоносному децентрализованному приложению распоряжаться криптовалютой;

3. Хищение криптовалюты совершено в результате хакерской атаки на децентрализованное приложение, если потерпевший разместил свою криптовалюту в этом приложении.

Аналогично, как и с хакерскими атаками на биржи, о взломе децентрализованных приложений появится соответствующая информация в официальных источниках, в частности, в социальной сети «Х» (запрещенная на территории Российской Федерации социальная сеть).

Если похищенная криптовалюта хранилась на некастодиальном кошельке и потерпевший сам произвел перевод криптовалюты, выдвижение версии о способе хищения происходит также, как если бы криптовалюта хранилась на кастодиальном кошельке. Единственным отличием является то, что хищение не могло произойти в результате взаимодействия с peer-to-peer платформой. Однако при хранении криптовалюты на некастодиальном кошельке существуют другие широко распространенные способы, при которых заявитель (потерпевший) самостоятельно совершает неравноценный обмен криптовалюты (обменивает на поддельные токены) или размещает свою криптовалюту на вредоносных децентрализованных приложениях, в результате чего происходит хищение.

После выдвижения и проверки вышеуказанных версий, возможно выдвинуть две типичные следственные версии о лице, совершившем хищение, по признаку связи с потерпевшим:

1. Хищение совершено посторонним для потерпевшего лицом.

2. Хищение совершено знакомым потерпевшему лицом или по его наводке.

Выдвижение первой версии наиболее целесообразно, если хищение произошло в результате хакерской атаки на биржу или децентрализовнное приложение, а также в случаях, когда потерпевшим дано разрешение вредоносному децентрализованному приложению распоряжаться криптовалютой. Ту же самую версию следует выдвинуть в случаях хищения в результате получения третьими лицами доступа к криптовалюте, когда потерпевший лично передал конфиденциальную информацию, позволяющую получить доступ к криптовалюте (логин и пароль, мнемоническую фразу, приватные ключи) в результате фишинга или взаимодействия с незнакомыми лицами. Аналогичная версия подлежит выдвижению и в случае, когда потерпевший лично взаимодействовал с незнакомым ему лицом посредством сети Интернет и осуществил перевод своей криптовалюты на чужой публичный адрес.

Вторую версию следует выдвинуть в случаях, когда криптовалюта украдена в результате получения к ней доступа третьими лицами, которые, например, имели доступ к устройствам, где хранилась криптовалюта, или знали о местах хранения данных, позволяющих получить доступ к криптовалюте. Это могут быть родственники, друзья, знакомые, работники и т.д. Выдвижение данной версии очевидно и при мошенническом хищении знакомыми потерпевшему лицами.[49]

[49] См. например: приговор Тимирязевского районного суда города Москвы от 17.09.2024 по делу № 1-320/2024, приговор Самарского гарнизонного военного суда от 18.11.2022 № 1-67/2022 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 14.06.2025).

Нельзя оставить без внимания версию о том, что заявитель добросовестно заблуждался относительно совершения хищения.

Желательно установить факт добросовестного заблуждения относительно совершения хищения на стадии проверки сообщения о совершенном преступлении. Однако это может не удастся сделать ввиду сжатых сроков и высокой загруженности следователей (дознавателей).

Поэтому данной версии в ходе предварительного расследования необходимо уделить особое внимание, поскольку при взаимодействии с криптовалютой пользователи часто теряют средства не только по вине злоумышленников, но и ввиду собственной неосмотрительности, отсутствия должных знаний, навыков, опыта и высокой концентрации внимания. Пользователь может совершить ошибку при совершении транзакции, указав ошибочный публичный адрес или выбрав неверный блокчейн. Именно поэтому следует выдвинуть данную версию в случае, когда транзакция инициирована заявителем При ошибочном указании публичного адреса криптовалюта поступит не на тот кошелек, либо будет утеряна, если такого адреса не существует. При неправильном выборе блокчейна, криптовалюта будет безвозвратно утеряна, если на неверно выбранном блокчейне не существует указанного публичного адреса. Так, например, если пользователь решил отправить USDC, находящийся на блокчейне «Tron» (TRC-20), в адрес другого кошелька, направлять нужно на кошелек в блокчейне «Tron» (TRC-20). Если попытаться направить одноименный актив на кошелек другого блокчейна (например, «Arbitrum One»), без использования специального децентрализованного приложения (моста), средства будут утеряны навсегда.

Установить вышеуказанные факты и обстоятельства возможно в ходе получения объяснений и осмотров блокчейн-обозревателей и криптовалютных кошельков.

Также примерами добросовестного заблуждения неопытного пользователя могут быть случаи, связанные с отсутствием необходимых знаний при использовании кошельков и децентрализованных приложений.

Некоторые криптовалютные кошельки, в силу своих особенностей, не отображают полный баланс всех имеющихся на них средств. Так, например, популярный криптовалютный кошелек «Metamask» не отображает баланс отдельных криптовалют до тех пор, пока пользователь не произведет соответствующую настройку вручную. Некоторые криптовалютные кошельки отображают баланс в рамках одного или нескольких блокчейнов, либо не отображают баланс в рамках отдельных блокчейнов. Например, вышеуказанный «Metamask» не отображает баланс BTC на блокчейне «Bitcoin», так как не предназначен для работы в указанном блокчейне. Факт наличия криптовалюты на кошельке возможно установить в ходе его осмотра. Если следователь (дознаватель) не обладает необходимыми знаниями и навыками, чтобы проверить наличие криптовалюты, необходимо произвести осмотр с привлечением лица, обладающего соответствующими знаниями.

При совершении криптовалютных транзакций пользователи оплачивают стоимость комиссий, размер которой зависит от выбранного блокчейна и нагрузки на него. В отдельные периоды времени комиссия в блокчейне «Ethereum» (ERC-20) может достигать более 100 долларов США. Пользователь может не заметить этого и совершить транзакцию, оплатив высокую стоимость комиссии. Наиболее распространен случай, когда пользователь, настраивая размер комиссии вручную, необоснованно занижает его. В результате средства списываются с баланса, но транзакция не валидируется по причине того, что майнеры (валидаторы) обрабатывают ее одной из последних, так как ее немедленная валидация представляется экономически нецелесообразной.

Отдельно можно выделить случаи, когда пользователи совершают сделки при помощи централизованной биржи или децентрализованных приложений, суть которых заключается в займе криптовалютных активов под залог собственной криптовалюты, с целью получить финансовую выгоду в результате роста или падения цены на отдельные криптовалютные активы. Обычно указанные сделки совершают пользователи, имеющие опыт

взаимодействия с криптовалютой, биржами и децентрализованными приложениями. Однако не редки случаи, когда неопытные пользователи заключают такие сделки без полного осознания возможных рисков и последствий, должного анализа и (или) в результате воздействия третьих лиц. В большинстве случаев, вышеуказанные лица теряют свои средства в результате их принудительного изъятия в тот момент, когда их залог перестает обеспечивать задолженность. Такое принудительное изъятие является не преступлением, а вероятным последствием вышеуказанных сделок. Подобные факты возможно установить в ходе осмотров блокчейн-обозревателей и криптовалютных кошельков.

Аналогичная ситуация может сложиться в результате гражданско-правовых отношений, когда исполнитель по договору получил от заказчика криптовалюту в управление и обязался принести прибыль, но исполнитель не выполнил свои обязательства ввиду неудачно совершенных сделок.

По изученным уголовным делам, в одном из апелляционных определений суда отменен обвинительный приговор суда первой инстанции, согласно которому подсудимый заключил с потерпевшим договор, предметом которого являлось управление криптовалютой потерпевшего, с целью получения последним прибыли, и в результате неудачно заключенных подсудимым сделок криптовалюта была утеряна (принудительно изъята в счет погашения задолженности).[50]

То же самое следует отметить про случаи, когда пользователь покупает криптовалютные активы по рекомендации третьих лиц или дублирует их действия (блогеров, знакомых и т.д.), а стоимость приобретенной криптовалюты снижается ввиду неблагоприятной рыночной конъюнктуры. Часто встречаются случаи, когда пользователи повторяют те действия, которые демонстрируют другие пользователи на широкую публику, выражая

[50] Апелляционное определение Московского городского суда от 14.10.2025 по делу № 10-19905/2025 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 14.11.2025).

свои мнения о перспективах роста цены на отдельные криптовалютные активы.

Таким образом, выдвижение типичных следственных версий следует начать с выяснения обстоятельств, при которых совершена транзакция, повлекшая хищение (совершил ли транзакцию сам потерпевший или же злоумышленник), а также с выяснения способа хранения криптовалюты. Знание ответов на эти два вопроса позволит выдвинуть более продвинутые версии и проверить их на жизнеспособность. При этом следует проверить версию о добросовестном заблуждении относительно совершения хищения. Следственная ситуация, в большинстве случаев, редко может быть благоприятной ввиду «дистанционного» характера хищения[51], отсутствия привязки криптовалютных кошельков к личности, а также использования злоумышленником средств анонимизации.

2.3. Взаимодействие следователя с органами, осуществляющими оперативно-розыскную деятельность

Теоретической основой исследования проблем взаимодействия органов предварительного расследования с органами, осуществляющими оперативно-розыскную деятельность, являются работы ряда ученых, посвятивших свои труды вышеуказанным вопросам.[52]

---

[51] Варданян А.В. Проблема систематизации цифровых методов оперативно-розыскной деятельности, используемых в борьбе с дистанционными хищениями, и их криминалистическое значение // Юрист-Правоведъ. 2022. № 2 (101). С. 8.

[52] См. например: Зеленский В.Д. Криминалистические проблемы организации расследования преступлений: дис. … д-ра юрид. наук: 12.00.09. Краснодар, 1991. 323 с, Земскова А.В. Теоретические основы использования результатов оперативно-розыскной деятельности при расследовании преступлений: дис. … д-ра юрид. наук: 12.00.09. Москва, 2002. 423 с, Зникин В.К. Научные основы оперативно-розыскного обеспечения раскрытия и расследования преступлений: дис. … д-ра юрид. наук: 12.00.09. Нижний Новгород, 2006. 442 с, Аменицкая Н.А. Взаимодействие следователя и органов, осуществляющих оперативно-розыскную деятельность в раскрытии и расследовании преступлений (в ОВД): дис. … к-та юрид. наук: 12.00.09. Нижний Новгород, 2006. 201 с, Нечаев В.В. Организационно-правовые основы взаимодействия органов предварительного следствия и дознания: автореферат дис. ... к-та юрид. наук: 12.00.11. Рязань, 2005. 26 с, Варданян А.В.,

Организационными формами взаимодействия с органами, осуществляющими оперативно-розыскную деятельность, являются:

1. Взаимодействие и координация действий между подразделениями органов внутренних дел: следователями, оперативниками и экспертами-криминалистами;

2. Взаимодействие при анализе собранных сведений, полученных в рамках производства следственных действий и оперативно-розыскных мероприятий;

3. Составление плана расследования, в том числе производства следственных действий и оперативно-розыскных мероприятий;

4. Обмен значимой информацией по материалу проверки или возбужденному уголовному делу.[53]

Используя лишь собственные возможности, следователь (дознаватель) не в состоянии выполнить свои задачи на первоначальном этапе расследования уголовных дел по фактам хищений криптовалюты. По этой причине ему необходимо обращаться за помощью к органам, осуществляющим оперативно-розыскные мероприятия. Применительно к делам о дистанционном хищении криптовалют такая помощь необходима как для производства следственных и иных процессуальных действий ими самостоятельно, участия в оказании содействия следователю при производстве следственных и иных процессуальных действий, так и для розыска обвиняемого, местонахождение которого неизвестно.

Плясов К.А. Оперативно-розыскное обеспечение предупреждения, раскрытия и расследования преступлений в сфере внешнеэкономической деятельности // Юристъ Правоведъ. 2022. № 1 (100). С. 94-99, Халиков, А. Н. Оперативно-розыскная деятельность : учебник / А.Н. Халиков. – 3-е изд. – Москва : РИОР : ИНФРА-М, 2024. – 331 с и др.

[53] Фарахиев Д.М. Деятельность органов внутренних дел в процессе раскрытия и расследования преступлений, совершаемых с использованием информационно-коммуникационных технологий (на примере криптовалютных активов) // Юридический вестник Самарского университета. 2023. № 3(9). С. 84.

Однако особенно востребована помощь оперативно-розыскных органов, когда необходимо установить личность владельца кошелька, куда поступили средства в результате хищения.

В одном из изученных уголовных дел, возбужденном по факту мошеннического хищения криптовалюты, видно, что на сегодняшний день органы предварительного расследования в поручениях, адресованных оперативно-розыскным органам, указывают на необходимость проведения периодической сверки реквизитов по подсистеме ИБД-Ф «Дистанционное мошенничество» на предмет совпадений с раскрытыми преступлениями. Анализ содержащейся в базе данных информации свидетельствует о возможности установить сведения о причастности уличенного в совершении преступления лица к совершению иных преступлений в сфере информационно-телекоммуникационных технологий с использованием им тех же номеров телефонов, банковских карт, адресов используемых сайтов и т.д.

Таким образом, при установлении лица, совершившего хотя бы один преступный эпизод с использованием тех же средств, возможно отследить и иные совершенные им преступления в любом регионе страны. Также в поручении указывается на необходимость оказания содействия в подготовке запросов в адрес кредитно-финансовых учреждений, операторов связи и иных организаций и учреждений, с целью истребования информации, способствующей раскрытию преступления; оказания содействия в проведении анализа полученной от вышеуказанных организаций информации и внесения предложений для включения в план совместных следственных действий и ОРМ; установления оперативным путем принадлежности абонентского номера, IP-адреса устройств, использованных для совершения звонков, и их принадлежность; в случае установления лиц, которым принадлежат указанные абонентские номера и IP-адреса, провести ОРМ на предмет их причастности к

совершенному преступлению; истребования справок ИЦ о ранее судимых по аналогичным статьям, проверить их причастность к данному преступлению.[54]

На наш взгляд, ту часть вышеуказанных действий, которая подразумевает направление запросов, необходимо производить органу предварительного расследования, поскольку следователь (дознаватель) не лишен такой возможности исходя из процессуального законодательства. Органам, осуществляющим оперативно-розыскные мероприятия, из всего перечисленного следует оставить сверки реквизитов по подсистеме ИБД-Ф «Дистанционное мошенничество» на предмет совпадений с раскрытыми преступлениями, а также установление оперативным путем принадлежности абонентского номера, IP-адреса устройств, использованных для совершения звонков, и их принадлежность; в случае установления лиц, которым принадлежат указанные абонентские номера и IP-адреса, провести ОРМ на предмет их причастности к совершенному преступлению.

Следует отметить, что по вышеуказанному уголовному делу установлены лица, причастные к хищению, но не задержаны. Не умаляя важность перечисленных в материалах данного уголовного дела действий, порученных оперативно-розыскным органам, считаем, что в условиях полного или частичного отсутствия информации о лицах, совершивших хищение, следует осуществить оперативно-розыскные мероприятия (наведение справок, опрос, исследование документов), направленные на поиск возможностей по установлению личности подозреваемого путем анализа транзакций в блокчейн-обозревателях, а затем на установление личности подозреваемого путем направления запросов.

Верно отмечено Перовым В.А., что необходимо определить те границы, где анонимность криптовалюты заканчивается и начинаются так называемые точки доступа к персональным данным определенного лица, совершающего

[54] Уголовное дело № 12401270015001224 СУ МВД России по г. Уфе.

криптовалютные операции, нарушающие требования национального законодательства.

Учитывая, что криптокошельки, как правило, являются анонимными, одной из таких «точек доступа» может являться операция по обмену (купле-продаже) той или иной криптовалюты на национальную валюту. Именно при совершении данной операции, осуществляемой путем зачисления фиатных денежных средств на банковский счет (списания со счета) лица, продавшего (приобретшего) криптомонеты, появляется возможность установить участника такой сделки или, по крайней мере, лицо, действующее в его интересах или с ним связанное определенными отношениями.

Второй «точкой доступа», хотя и не всегда позволяющей точно персонифицировать лицо, совершающее противозаконные сделки с криптовалютой, но при этом все же позволяющей сделать относительно определенные предположения относительно такого лица, является комплексный анализ информации о связях анонимного лица с уже ранее реально установленными лицами, а также анализ информации анонимных и реальных лиц, в том числе в телекоммуникационной сети Интернет.[55]

Действительно, в большинстве случаев, криптовалютный кошелек взаимодействовал или будет взаимодействовать с другими кошельками до и после совершения хищения, соответственно. Наличие связи возможно обнаружить в ходе осмотров блокчейн-обозревателей. Цели таких взаимодействий могут быть разными. Одна их самых распространенных – обналичить похищенную криптовалюту при помощи peer-to-peer платформы или обменников. В первом случае криптовалюту необходимо перевести на кошелек, принадлежащий бирже. Большинство криптовалютных бирж требует верификации личности пользователя путем предоставления фамилии, имени,

[55] Перов В.А. О криминалистической методике выявления преступлений, совершаемых с использованием криптовалюты, и расследовании соответствующих уголовных дел // Российский следователь. 2020. № 12. С. 10-13. [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 14.06.2025).

отчества, даты рождения, фотографии и официальных документов. Однако следует иметь ввиду, что лицо, прошедшее верификацию, фактически, может не пользоваться биржевым аккаунтом и не быть причастным к хищению. Обменники могут совершать обмены как с помощью банковского перевода, так и наличными. Если обмен совершен с помощью банковского перевода, существует вероятность того, что такому обмену предшествовала подача заявки на обмен через официальный сайт обменника. Это означает, что лицо, осуществлявшее обмен, оставило информацию о своем IP-адресе, по которому возможно установить провайдера услуг, а также страну, город нахождения и другую важную информацию. Наличный обмен, с одной стороны, позволяет сохранить большую конфиденциальность, с другой – обменник предоставляет адрес своего нахождения желающим совершить наличный обмен, что позволяет следователю (дознавателю) во взаимодействии с оперативно-розыскными органами прибыть по месту нахождения обменника и совершить необходимые следственные действия, с целью установления лица, которому принадлежит кошелек, получивший похищенную криптовалюту. Однако в этом случае необходимо обладать информацией о том, в каком городе совершен обмен, если обменник функционирует в нескольких городах.

Анализ судебной практики показал, что выявить личность преступников оперативно-розыскным органам удалось в результате действий, направленных на установление: принадлежности кошельков-получателей похищенных средств конкретной бирже; личностей, на чьи имена зарегистрированы биржевые аккаунты; IP-адресов, выданных электронным носителям информации, использованным для совершения преступлений; провайдеров, обслуживавших данные IP-адреса; адреса проживания и данных о личностях, выступавших сторонами по договорам оказания услуг по предоставлению доступа в Интернет. В результате проведенных оперативно-розыскных

мероприятий преступники были задержаны, а позже была установлена и доказана их причастность и вина в совершении хищений.[56]

Взаимодействия кошелька до совершения хищения также могут быть важны для предварительного расследования, поскольку пользователь этого кошелька мог взаимодействовать с кошельками, принадлежащими биржам или обменниками, с целью купить криптовалюту. Наличие таких фактов также повышает вероятность установления личности подозреваемого.

Формируя поручения для оперативно-розыскных органов в вышеуказанных условиях, 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.

Если в ходе оперативно-розыскных мероприятий удалось установить принадлежность какого-либо из кошельков обменнику, необходимо поручить проведение обыска по месту нахождения обменника. По результатам обыска появится возможность установить в ходе допросов и осмотров банковские

[56] См. например: приговор Первомайского районного суда города Краснодара от 17.04.2024 по делу № 1-212/2024, приговор Новгородского районного суда Новгородской области от 18.11.2024 № 1-947/2024 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 14.06.2025).

реквизиты лица, в чей адрес осуществлен перевод денежных средств в обмен на полученную криптовалюту.

Если вышеуказанная информация имеется, необходимо провести оперативно-розыскные мероприятия (исследование документов, опрос, наблюдение, наведение справок) в отношении владельцев кошельков, а также профилей, которые указали публичные адреса кошельков, в ходе которых необходимо установить: данные о личности, электронную почту, номер телефона, страну и адрес проживания, удостоверяющий личность документ, идентификатор социальной сети или мессенджера, IP-адрес при регистрации и входе в систему, геолокация мест входа, цифровой профиль использованного для входа устройства, данные о проведенных операциях и т.д.

Кроме того, следует поручить установление связи публичных адресов кошельков с публичными адресами кошельков, которые зафиксированы в соответствующих базах данных, имеющихся у оперативно-розыскных органов. В особенности это касается тех дел оперативного учета и уголовных дел, по которым установлены владельцы криптовалютных кошельков.

Для установления принадлежности криптовалютного кошелька криптовалютной бирже или обменнику существует ряд различных онлайн-сервисов.

В странах СНГ широкое применение получил сервис анализа криптовалютных транзакций «Прозрачный блокчейн», принадлежащий Российской Федерации в лице Росфинмониторинга, который предоставляется государственным и правоохранительным органам стран-партнеров бесплатно. Помимо функций отслеживания и визуализации транзакций, он обладает собственной аналитической моделью скоринговой оценки и уникальной базой данных криптокошельков, позволяет связать их с конкретными криптобиржами и обменниками. Сервис автоматически собирает и анализирует информацию из Интернета, включая соцсети и DarkNet, в режиме online, распределяет полученную информацию по заданным критериям. В актуальной версии «Прозрачный блокчейн» позволяет отслеживать

криптовалютные транзакции с использованием более 20 популярных криптовалют.

«Прозрачный блокчейн» содержит постоянно пополняемый список размеченных криптокошельков и участников транзакций с возможностью их фильтрации по принадлежности к противоправной деятельности, конкретным криптобиржам и обменникам. Пользователь может сохранить и загрузить информацию об адресе, его владельце или транзакции, которая будет видна только ему. С помощью программы можно получить отчеты на конкретные даты с разбивкой по времени и биржам, что необходимо для доказывания факта совершения преступления и определения стоимости предмета преступления.

На сегодняшний день «Прозрачный блокчейн» содержит самый широкий перечень функций в сравнении с аналогами, доступными пользователям большинства стран СНГ, и в условиях пробелов в правовом регулировании является эффективным инструментом отслеживания криптовалютных транзакций, позволяющим установить владельцев криптокошельков.[57]

Для выявления фактов упоминания криптовалютного кошелька в сети Интернет, следует воспользоваться методом прямого соотнесения данных о принадлежности криптовалютного кошелька.

Для этого, в частности, используется поиск упоминаний проверяемых криптокошельков в поисковых системах Яндекс, Google или Даркнет-поисковиках. Сведения о принадлежности криптокошельков могут быть опубликованы на различных Интернет и Даркнет сайтах, в форумах, блогах, социальных сетях, документах Google Docs, а также в специализированных сервисах-отзовиках.

[57] Тисен О.Н. Методика обнаружения, фиксации и изъятия электронно-цифровых следов по делам о преступлениях, совершенных с использованием криптовалют // Уголовное право. 2024. № 3. С. 69-80. [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 14.06.2025).

Отнесение криптокошелька к бирже, обменнику или иному сервису, использующему цифровую валюту, возможно при помощи таких ресурсов, как: walletexplorer.com, bitinfocharts.com, oxt.me. Они также позволяют извлекать (методом парсинга) массивы информации для использования в собственных аналитических системах. Парсинг представляет собой метод собирания и систематизации информации, размещенной на определенных сайтах, с помощью специальных программ, автоматизирующих процесс. Задача последних – синтаксический анализ, разбор поступающей информации, ее структурирование. Иными словами, парсинг направлен на получение необходимых данных, соответствующих заданным параметрам.

Установление связи между покупкой криптовалюты конкретным лицом и зачислением схожего числа криптовалюты на один из криптовалютных кошельков обеспечивается выявлением следующих цифровых идентификаторов: никнейм, фотография, IP-адрес, адрес электронной почты, номер мобильного телефона, цифровой профиль устройства и др.

Никнейм (англ. nickname) – это псевдоним, применяемый пользователем в Интернете обычно в местах общения (блогах, форумах, чатах, социальных сетях, мессенджерах и электронной почте). Поиск совпадений по никнейму в сети Интернет проводится путем использования следующих сервисов: namechk.com, whatsmyname.app, instantusername.com, infotracer.com, intelx.io/tools?tab=username, go.mail.ru/search_social или t.me/maigret_osint_bot.

Фотография пользователя также может быть использована для установления личности путем ее сопоставления с существующими базами биометрических данных социальных сетей.

Наиболее распространенными сервисами для этого являются: findclone.ru, search4faces.com, pimeyes.com. Для решения данной задачи можно использовать штатные возможности поисковых сервисов: yandex.ru/images, go.mail.ru/search_images и images.google.com.

IP-адреса анализируются на предмет принадлежности к конкретному региону и использования средств анонимизации сетевого трафика. Для этого

можно использовать следующие ресурсы: maxmind.com/en/geoip2-precisiondemo, sypexgeo.net/ru/demo/ или ipinfo.io/map.

Номер мобильного телефона и адрес электронной почты – это одни из самых распространенных идентификаторов, используемых в качестве средства подтверждения входа или двухфакторной идентификации в большинстве онлайн-сервисов и приложений. В российском сегменте Интернета функционирует значительное количество специализированных сервисов, позволяющих проводить автоматизированную проверку номеров телефонов и адресов электронной почты. К ним относятся: ТелПоиск, Инфосфера, NEO, Прима Информ, IDX, Spectrum Data и др.

Получение цифрового профиля устройства пользователя осуществляется посредством перенаправления его трафика на подконтрольный web-ресурс. Таким ресурсом может являться сайт в сети Интернет, на котором были заранее размещены специальные скрипты, предназначенные для идентификации посетителей. Существуют также общедоступные интернет-логгеры, такие как: iplogger.ru, grabify.link или canarytokens.org. Они позволяют пользователю создать уникальную ссылку на тот или иной объект в Интернете, проходя по которой пользователь оставит данные о своем устройстве.[58]

Однако, несмотря на наличие положительного опыта, проблем выявления, раскрытия преступлений, совершаемых с использованием криптовалюты, остается множество, в том числе процессуального, криминалистического, организационного и технического характера. Среди прочих к ним можно отнести:

– отсутствие достаточных знаний у сотрудников правоохранительных органов в целом о криптовалюте и ее техническом «скелете»;

[58] Гаврилин Ю.В., Бедеров И.С. Установление личности владельцев цифровой валюты: методологические основы // Труды Академии управления МВД России. 2021. № 4(60). С. 105-106.

– недостаточная проработанность законодательства и некоторых положений, в особенности это касается терминологии («цифровые права», «цифровые активы», «цифровая валюта», «криптовалюта», «виртуальная валюта»);

– несовершенство отечественных аппаратно-программных комплексов, позволяющих получать информацию с различных электронных носителей на которых, в том числе хранится криптовалюта;

– ограниченное количество компетентных экспертов и специалистов в области компьютерно-технических экспертиз, в том числе как в ведомственных государственных учреждениях, так и в негосударственных организациях;

– отсутствие эффективного международного сотрудничества в части обмена информацией, а также отсутствие регулирования и контроля над провайдерами услуг.

Для эффективного противодействия преступлениям, связанным с дистанционным хищением криптовалюты, необходима модернизация методов оперативно-розыскной деятельности. Это включает внедрение аналитических инструментов для отслеживания транзакций, активное использование OSINT-методов и сотрудничество с криптовалютными биржами, которые внедряют процедуры верификации пользователей (KYC).

Кроме того, необходимо создание специализированных подразделений в структурах правоохранительных органов, обладающих компетенцией в области цифровых финансов и блокчейн-аналитики.

Повышение квалификации сотрудников ОРД, а также следователей и дознавателей, внедрение новых технологий и активное международное взаимодействие являются ключевыми направлениями в противодействии преступлениям, связанным с криптовалютами.

Анализ позволяет сделать вывод, что использование криптовалют в целях совершения преступлений является серьезной правовой проблемой,

которая требует творческих, находчивых и совместных подходов к правоприменению и регулированию. Для эффективного выявления и раскрытия преступлений, совершаемых с использованием криптовалют, необходима всеобъемлющая нормативно-правовая база и использование передовых аналитических технологий.

Ключевую роль играет и международное сотрудничество, поскольку зачастую криптобиржи находятся за пределами нашего государства. Обмен информацией между правоохранительными органами разных стран, создание совместных оперативных групп и единых стандартов регулирования позволит повысить эффективность борьбы с криптовалютными преступлениями. В связи с этим, правоохранительным органам важно активно регулировать и вести строгий надзор за провайдерами услуг по управлению виртуальными активами. Интеграция надзора в России может осуществляться в форме сотрудничества между правоохранительными органами и финансовыми регуляторами, обеспечивающего эффективное и скоординированное правоприменение.[59]

[59] Рощупкина А.В. Специфика криптовалют для целей оперативно-розыскной деятельности // Вестник Удмуртского университета. 2025. № 3(35). С. 530.

Глава 3. Тактические особенности производства отдельных следственных действий на первоначальном этапе расследования дистанционных хищений криптовалютных активов

3.1. Особенности производства следственного осмотра

Событие преступления имеет сущность, которая может проявиться в окружающем мире – все отображается.[60] В силу специфики технологии блокчейн, объективная информация, позволяющая получить достоверные доказательства о событии предполагаемого хищения, отображается в истории транзакций криптовалютного кошелька и блокчейн-обозревателях. Поэтому осмотр является ключевым следственным действием на первоначальном этапе расследования хищений криптовалюты, поскольку именно благодаря нему есть возможность достоверно установить наличие тех или иных фактов и обстоятельств, проверить объяснения и показания допрошенных, а также выдвинуть следственные версии по поводу отдельных элементов совершенного преступления и развивать дальнейший ход расследования.

По нашему мнению, основными объектами осмотра в рамках осмотров электронных носителей информации являются криптовалютные кошельки и блокчейн-обозреватели, поскольку они отражают записи, произведенные в блокчейне, которые, в большинстве случаев, неизменны.

Их осмотр позволит получить достоверную информацию о совершенных транзакциях, времени их совершения и суммах, а также идентифицировать публичные адреса кошельков, с которыми взаимодействовал осматриваемый кошелек. Полученная в ходе осмотра информация позволит произвести ряд других процессуальных действий, в результате которых может быть идентифицирована личность

[60] Руденко А.В. Мыслительная деятельность следователя (дознавателя) при поиске следов преступления // Юридический вестник Кубанского государственного университета. 2015. № 1 (22). С. 18.

злоумышленника или лиц, которые каким-то образом связаны со злоумышленником.

Примечательно то, что блокчейн-обозреватель может быть осмотрен с любого персонального компьютера (в том числе и с планшетного компьютера, и со смартфона), если известен публичный адрес кошелька и наименование блокчейна. Это позволяет произвести осмотр без каких-либо выездов и изъятий электронных носителей информации, сразу после получения объяснения (допроса). То же самое можно сказать и о криптовалютном кошельке, если имеется информация о входных данных, либо предоставившее объяснение (допрошенное) лицо имеет доступ к кошельку через устройство, которое находится при нем, и он готов представить его на обозрение.

Возможность осмотра криптовалютного кошелька существенно облегчает ход расследования, поскольку в истории транзакций возможно обнаружить транзакцию, в результате совершения которой произошло хищение. В связи с тем, что транзакции в истории кошелька хранятся ограниченное количество времени, и следователь (дознаватель) не всегда имеет к нему доступ, осмотр рекомендуется проводить посредством блокчейн-обозревателя.

Для проведения осмотра посредством блокчейн-обозревателя необходим один из трех идентификаторов:

1. ID транзакции;
2. Публичный адрес кошелька отправителя;
3. Публичный адрес кошелька получателя.

ID транзакции является наилучшим вариантом, поскольку сразу откроет страницу с транзакцией, в результате которой совершено хищение. При наличии лишь публичного адреса необходимо дополнительно искать вышеуказанную транзакцию.

Если заявитель по каким-то причинам располагает информацией о публичном адресе кошелька получателя, но не располагает информацией о публичном адресе собственного кошелька и его невозможно установить,

необходима информация о дате и времени, когда совершена транзакция, в результате которой произошло хищение, либо был обнаружен факт хищения, а также наименование криптовалюты и сумма, которая была похищена. Это позволит сузить поиск искомой транзакции.

В этом случае для осмотра через блокчейн-обозреватель желательно обладать информацией о том, в каком блокчейне совершена транзакция. Если получить информацию о блокчейне по каким-либо причинам не представляется возможным, следует воспользоваться специальными онлайн сервисами. К числу таких обозревателей относятся: blockchair.com, tokenview.com, blockchain.com, bitaps.com и live.blockcypher.com. Если такой поиск не дал результатов, следует проверить наличие искомой транзакции во всех возможных блокчейн-обозревателях.

Для наглядности приведем несколько примеров того, как выглядят транзакции в одном из блокчейн-обозревателей.

Обладая информацией о публичном адресе владельца криптовалютного кошелька и введя его в поисковую строку, мы увидим весь список транзакций, совершенный с адреса данного кошелька в рамках одного блокчейна (Приложение 2). Так, например, в Приложении 3 можно увидеть, как выглядит транзакция по переводу средств с одного публичного адреса на другой. В левом верхнем углу указано слово «Transfer», по которому можно сделать вывод, что это транзакция по переводу средств. Далее указано количество и наименование криптовалюты, а также публичный адрес получателя. Ниже указаны ID транзакции, статус выполнения, дата и время совершения, публичные адреса отправителя и получателя, наименование и количество переведенной криптовалюты и криптовалюты, уплаченной в качестве комиссии для валидаторов с долларовым эквивалентом на момент совершения транзакции. В Приложении 4 можно увидеть, как выглядит транзакция по предоставлению разрешения на распоряжение криптовалютой децентрализованному приложению. В левом верхнем углу указано «Approve Unlimited», что означает предоставление безлимитного разрешения на

распоряжение криптовалютой. Далее указано наименование криптовалюты, которой разрешено распоряжаться; наименование децентрализованного приложения, которому предоставлено разрешение и публичный адрес, который предоставил разрешение. Ниже указана та же информация, что и в ранее описанной транзакции.

Не следует пренебрегать иными объектами осмотра. Однако исходить следует из ранее полученных объяснений от потерпевшего и результатов осмотра блокчейн-обозревателя и криптовалютного кошелька. Если показания потерпевшего подтверждаются в ходе вышеуказанных осмотров, необходимо осмотреть те объекты, о которых упоминал потерпевший (заявитель) в ходе допроса (получения объяснения). В зависимости от обстоятельств хищения объектами осмотра могут быть истории посещений браузеров (особое внимание следует обратить на историю посещений 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. Если имеются основания полагать, что хищение произошло в результате работы вредоносного программного обеспечения, следует изъять электронные носители информации с участием специалиста в компьютерно-технической области для назначения компьютерно-технической экспертизы.

В ходе осмотра электронных устройств необходимо обращать внимание на следующие электронные следы:

– письма с криптобирж и обменников;

– наличие в истории браузера поисковых запросов криптовалютной тематики;

– письма из службы поддержки криптобирж и обменников;

– следы хранения сведений об открытых и закрытых ключах (в устройствах могут храниться файлы с сохраненными паролями доступа, открытыми и приватными ключами);

– переписку потерпевшего со злоумышленником.

Перед проведением осмотра целесообразно наладить взаимодействие со специалистами для получения консультативной помощи и помощи во время непосредственного осмотра. Приглашая специалиста, следователь (дознаватель) должен удостовериться, что последний имеет необходимое техническое и программное оснащение для работы с компьютерной информацией (ее копирования, создания образа носителя). Такими специалистами могут выступать как сотрудники экспертно-криминалистических подразделений правоохранительных органов, так и специалисты негосударственных аналитических компаний, специализирующихся на безопасности цифровых активов[61], например, АО «ШАРД».[62] К осмотру электронных носителей информации следует привлекать специалистов в сфере компьютерной информации, а также обладающих практическими навыками по взаимодействию с технологией блокчейн и криптовалютой. С одной стороны, это необходимо для случаев изъятия электронных носителей информации и копирования с них информации, так как того требует действующее уголовно-процессуальное законодательство. С другой стороны, участие специалиста необходимо для эффективного поиска и изъятия нужных электронных носителей информации, поиска, копирования и изъятия необходимой информации внутри найденных носителей информации, а также для правильной расшифровки записей (транзакций) в блокчейн-обозревателях.

Также в ходе предварительного расследования целесообразно повторять

[61] Осипов Г.П. Изъятие и арест криптовалюты: роль и участие специалиста // Вестник Университета прокуратуры Российской Федерации. 2025. № 3 (107). С. 93.

[62] АО «ШАРД»: сайт. URL: https://shard.ru/services/crypto-investigations (дата обращения: 07.12.2025).

совершенные осмотры блокчейн-обозревателей, потому что злоумышленники могут распорядиться похищенным не сразу, а спустя какое-то время, о чем в блокчйн-обозревателе появится информация.

Что касается осмотра криптовалютного кошелька, в большинстве случаев, он хранится в виде программы или браузерного расширения на смартфоне или персональном компьютере. Реже, кошелек хранится в виде аппаратного устройства, флеш-накопителя, пластиковой карты, а также в виде других предметов. Доступ к биржевому аккаунту обеспечивается через программное обеспечение или сайт в сети Интернет. У любых современных криптовалютных кошельков, а также в личных кабинетах централизованных бирж есть возможность просмотра истории всех совершенных транзакций с кошелька, а также поступления средств на кошелек, где имеется информация о кошельках, в адрес которых совершена транзакция или которые направили средства на осматриваемый кошелек, ID транзакциях, времени их совершения, а также наименованиях криптовалюты, которая была отправлена или получена.

Как мы указали выше, любую из таких транзакций возможно проверить через блокчейн-обозреватель, чтобы окончательно убедиться в ее подлинности. Для этого можно скопировать ID транзакции и вставить его в поле для поиска на сайте блокчейн-обозревателя. В некоторых кошельках ID транзакции является кликабельной ссылкой, при нажатии на которую происходит перенаправление на сайт блокчейн-обозревателя.

Важно помнить, что любое программное обеспечение, являющееся криптовалютным кошельком – это интерфейс для воспроизведения информации, содержащейся на кошельке. Любой кошелек возможно воспроизвести при помощи любого программного обеспечения, являющегося криптовалютным кошельком. Чтобы воспроизвести кошелек на любом другом программном обеспечении, необходимо ввести мнемоническую фразу или приватный ключ. При этом некоторые программы предназначены для работы только с определенными блокчейнами. Так, например, кошелек Metamask не

предназначен для работы с блокчейном «Bitcoin» и найти транзакции в этой сети при помощи кошелька «Metamask» не представится возможным. Однако это не значит, что пользователь не совершал транзакций в сети «Bitcoin» при использовании кошелька. Кошелек «Petra Wallet» предназначен только для работы на блокчейне «Aptos». Поэтому на данном кошельке не представится возможности отыскать транзакции, совершенные, к примеру, на, так называемых, «эфироподобных сетях» («Ethereum», «Arbitrum», «Optimism», «Base», «Unichain» и др.).

Если криптовалютный кошелек на изъятом устройстве по какой-либо причине не позволяет просмотреть историю транзакций, целесообразно воспроизвести этот кошелек через программное обеспечение, позволяющее просмотреть историю транзакций на любых или большинстве блокчейнов, – мультивалютный кошелек (например, Rabby Wallet или OKX Wallet). Данные кошельки также имеют функционал по отображению всех разрешений, данных децентрализованным приложениям, что очень информативно для предварительного расследования при производстве осмотра кошелька потерпевшего. Данная информация крайне полезна, если потерпевший не производил каких-либо переводов в адрес злоумышленников, но средства были похищены.

Если в ходе осмотра электронного носителя информации показания не подтверждаются или осмотр невозможен ввиду отсутствия необходимой информации (публичного адреса и (или) ID транзакции), наиболее эффективным будет проведение осмотра криптовалютного кошелька и блокчейн-обозревателя по месту нахождения потерпевшего (дом, квартира, офис и т.д.). В рамках такого осмотра можно обнаружить электронные носители информации, с которых есть доступ к криптовалютному кошельку, а также иную информацию, имеющую значение для дела. Еще одним преимуществом является возможность изъять устройства как для последующих осмотров, так и для назначения и проведения экспертиз.

Фиксации в протоколе подлежит весь процесс следственного действия с момента включения электронного устройства, наличие или отсутствие пароля, вид и содержание «рабочего стола», находящиеся на нем файлы, имеющие значение для дела, и их содержание, а также цепочка получения информации. При наличии на электронном устройстве специального программного обеспечения (приложения), используемого для совершения транзакций, целесообразно осмотреть приложение, баланс кошелька, сведения о нем, историю проводимых транзакций. Для сохранения информации о транзакциях на внешнем устройстве важно синхронизировать криптовалютный кошелек со смартфона с компьютером следователя. Веб-страницу с историей операций можно сохранить в виде отдельного файла, который должен быть приобщен к протоколу. Витрина ряда приложений может содержать вкладку «скачать транзакции», использование которой позволяет создать отчет о проводимых с использованием криптокошелька транзакциях и сохранить эти сведения в отдельном файле. Вся полученная информация должна быть сохранена, зафиксирована, подробно описана и приобщена к материалам дела.

Необходимо внимательно отнестись к идентификаторам (ID транзакций и публичным адресам кошельков), поскольку они состоят из большого количества латинских букв разного регистра и цифр. В ходе фиксации такой информации легко запутаться и допустить ошибку. Также следует сохранять на бумажном носителе и в электронном виде изображения тех страниц блокчейн-обозревателей и транзакций в кошельках, которые имеют значение для дела, и прилагать их к протоколу осмотра, чтобы легче воспринимать информацию в будущем. В тексте протокола осмотра целесообразно делать ссылки на приложения.

Все действия должностных лиц с криптовалютой должны быть пошагово зафиксированы в протоколе с приложением фототаблицы и (или) видеозаписи, при необходимости осуществляться с участием специалиста и (или) понятых.

Важно указать в протоколе марку, модель, тип и наименование устройств, которые использовались в ходе следственных действий. В процессуальных документах необходимо отразить реквизиты криптокошельков и криптовалюты, наименование и другие сведения о криптобирже/обменнике, сведения о транзакциях.

Таким образом, осмотр криптовалютных кошельков и блокчейн-обозревателей – 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.

3.2. Особенности допроса потерпевшего от хищения криптовалюты

Допрос является одним из важнейших следственных действий, производство которого необходимо не только по уголовным делам о хищении криптовалюты, но и, буквально, по всем уголовным делам, чтобы направить их на судебное рассмотрение.[63]

В силу специфики рассматриваемого преступления, личность

[63] Эксархопуло А.А., Макаренко И.А., Зайнуллин Р.И. Криминалистика : учебник для вузов / - Москва : Издательство Юрайт, 2025. - 477 с.

похитивших криптовалюту неизвестна не только потерпевшему, но и следователю (дознавателю). По этой причине, на первоначальном этапе расследования следователю (дознавателю) доступен допрос потерпевшего, который необходимо произвести, чтобы получить как можно больше криминалистически значимой информации.

Для успешного проведения допроса потерпевшего по делу о хищении криптовалютных активов следователю (дознавателю) необходимо знание, как минимум, понятийного аппарата о взаимодействии с криптовалютой. Об этой необходимости прямо или косвенно отмечают разные авторы работ, посвященных отдельным аспектам расследования преступлений, связанных с криптовалютой, с чем нельзя не согласиться.

Так, например, М.О. Янгаева утверждает, что «анализ практики расследования преступлений, связанных с использованием криптовалюты, показывает, что лица, осуществляющие расследование, не обладают в должной степени криминалистическими знаниями, необходимыми для расследования уголовных дел исследуемой категории, а также знаниями по тактике производства отдельных следственных и иных процессуальных действий. В этой связи ошибки и недочеты приводят к потере важной информации, следов, имеющих доказательственное значение».[64] И.А. Ишин также придерживается мнения, что сотрудники органов внутренних дел не всегда обладают достаточными познаниями в указанной сфере. Для решения проблемы он предложил ввести соответствующий спецкурс при подготовке курсантов и слушателей образовательных организаций МВД России, а также возложить на начальника органа дознания контроль за профессиональной компетентностью сотрудников, занимающихся расследованием преступлений, совершенных с использованием криптовалюты и иных высоких

[64] Янгаева М.О. Отдельные аспекты производства допросов при расследовании преступлений, связанных с использованием криптовалют // Материалы криминалистических чтений: научные основы противодействия (Долговские чтения): сб. материалов, Барнаул, 24 ноября 2022 г.: С. 90.

технологий, а также обязанность организации соответствующих курсов повышения квалификации для таких сотрудников.[65]

Одним из источников криминалистической методики расследования отдельных видов и групп преступлений выступает накопленный практический опыт, который в отношении хищений в сфере оборота криптовалют еще не имеет сформировавшейся и относительно устойчивой базы знаний ввиду отсутствия их систематизации и обобщения.[66] Отсутствие систематизации и обобщения базы знаний связано с относительно недавним появлением криптовалют и преступлений, направленных на их хищение. Поэтому у сотрудников правоохранительных органов отсутствует должный опыт в выявлении, пресечении и расследовании таких преступлений.[67]

Переходя к организационным особенностям, необходимо начать с того, что следует наладить взаимодействие со специалистами для получения консультативной помощи при подготовке к следственным действиям. Такими специалистами могут быть блокчейн и веб-разработчики со знанием различных языков программирования, блокчейн-инженеры, криптоброкеры, майнеры, специалисты по обеспечению кибербезопасности, системные администраторы, криптографы и другие.[68]

Помимо непроцессуального взаимодействия следует обратить внимание на возможность привлечения к участию специалиста в допросе, поскольку он может оказать следователю помощь в разъяснении специфической терминологии и постановке нужных вопросов.[69]

---

[65] Ишин И.А. Указ. соч. 2020. С. 85.

[66] Шнейдерова Д.И. Указ. соч. 2022. С. 158.

[67] Тисен О.Н. Специфика расследования преступлений, совершенных с использованием криптовалют // Новые, появляющиеся и видоизменяющиеся формы преступности: научные основы противодействия (Долговские чтения): сб. материалов II Всерос. науч.-практ., Москва, 24-25 марта 2022 г.: С. 173.

[68] Шнейдерова Д.И. Указ. соч. 2020. С. 105.

[69] Шнейдерова Д.И. Тактические особенности допроса подозреваемого по делам о хищениях в сфере оборота криптовалют // Борьба с преступность: теория и практика: материалы докладов XI Международной научно-практической конференции, Могилев, 07 апреля 2023 г.: С. 492.

Также это поможет выявить противоречия в показаниях потерпевшего и, в целом, оценить его уровень знаний и наличие опыта. Понимание уровня знаний и опыта потерпевшего позволит следователю (дознавателю) наиболее эффективно спланировать предварительное расследование. Опытный и знающий потерпевший своими показаниями способен существенно облегчить ход расследования.

Если потерпевший способен самостоятельно пояснить об обстоятельствах хищения, следует предоставить ему возможность дать показания в форме свободного рассказа вне зависимости от его знаний и опыта во взаимодействии с криптовалютой. После окончания дачи показаний в свободной форме необходимо задать уточняющие вопросы. Также для предварительного расследования эффективно и полезно, чтобы потерпевший продемонстрировал доказательства совершения транзакций из блокчейн-обозревателей и истории транзакций на кошельке, переписки с предположительными злоумышленниками и другие доказательства, достоверно подтверждающие его слова.

Поскольку криптовалютная сфера является относительно новой, многие пользователи имеют мало знаний и опыта в данной сфере. Поэтому в ходе допроса потерпевшие нередко будут не способны дать подробные объяснения об обстоятельствах хищения. Налаживание психологического контакта и правильно заданные вопросы могут помочь такому потерпевшему вспомнить обстоятельства и факты, имеющие значение для уголовного дела.

Первостепенной задачей будет являться выяснение:

– способа, при помощи которого потерпевший хранил похищенную криптовалюту (на кошельке централизованной биржи или на некастодиальном кошельке), наименование сервисов, которые он использовал для доступа к криптовалюте, а также наименование, идентификатор и количество похищенной криптовалюты, название блокчейна и публичный адрес, где хранилась криптовалюта;

– совершались ли транзакции на криптовалютном кошельке потерпевшего и производил ли он их лично;

– ID транзакции, если потерпевшему известно в результате совершения какой транзакции совершено хищение;

– способов покупки и продажи криптовалюты;

– с какой целью совершена транзакция, если ее совершил потерпевший;

– даты, времени, публичного адреса кошелька, на который осуществлен перевод;

– способа хранения данных, обеспечивающих доступ к криптовалюте;

– передавал ли потерпевший посторонним лицам, каким-либо Интернет-сайтам, браузерным расширениям, а также программным обеспечениям или приложениям вышеуказанные данные;

– наличия или отсутствия переписок с предполагаемым злоумышленником, их содержание, мессенджер или социальная сеть, при помощи которых состоялась переписка, а также данные, которые указал о себе предполагаемый злоумышленник;

– какие электронные носители информации, Интернет-сайты, программные обеспечения, браузерные расширения и (или) приложения использовал потерпевший для работы с криптовалютой;

– устанавливались ли для входа в программные обеспечения, браузерные расширения и (или) приложения, использовавшиеся для взаимодействия с криптовалютой, дополнительные меры защиты (пин-коды, Face ID, вход по отпечатку пальца, двухфакторная аутентификация и т.д.);

– круга лиц, которые потенциально имели доступ к электронным носителям информации потерпевшего, а также к данным, обеспечивающим доступ к криптовалюте, и имели возможность преодолеть вышеуказанные дополнительные меры защиты, если они были установлены;

– фактов выбытия из владения потерпевшего хотя бы одного из электронных носителей информации, с помощью которого осуществлялось взаимодействие с криптовалютой, и период времени такого выбытия;

– длительности работы потерпевшего с криптовалютой;

– направлений деятельности, которые потерпевший практиковал при работе с криптовалютой;

– на какой онлайн-контент он ориентировался при работе с криптовалютой;

– какие онлайн-ресурсы потерпевший посещал и что загружал на свои электронные носители информации незадолго до хищения;

– соединял ли электронные носители информации, которые использовались для работы с криптовалютой, с другими электронными носителями информации и устройствами, в том числе, с Wi-Fi источниками.

Четверть опрошенных респондентов придерживается мнения, что первоначальный этап расследования хищений криптовалюты должен быть начат с выяснения обстоятельств о способе хранения криптовалюты и инициаторе транзакции, повлекшей хищение. Половина затруднилась с ответом на вопрос (приложение 1).

Также необходимо предложить потерпевшему продемонстрировать истории транзакций на кошельке и в блокчейн-обозревателях, а также переписки со злоумышленниками и другие необходимые доказательства. Учитывая это, выбор места для проведения допроса определяется возможностью доступа к сети Интернет.[70]

Выяснение вышеизложенного, помимо того, что поможет выдвинуть следственные версии, даст больше понимания об уровне знаний и опыте потерпевшего. Чем ниже уровень знаний и опыт, тем, как правило, его допрос

[70] Мельник Л.Л. Подготовительный этап допроса подозреваемого при расследовании преступлений против собственности, совершенных с использованием криптовалют и электронных денег / Л.Л. Мельник // Сацыяльна-эканамічныя і прававыя даследаванні. 2023. № 1(71). С. 79.

может оказаться менее полезным для предварительного расследования с точки зрения установления обстоятельств, имеющих значение для уголовного дела, так как потерпевший вряд ли сможет пояснить о том, какие действия совершал и с какой целью, в результате чего могло быть совершено хищение. Вместе с тем, выше вероятность того, что потерпевший потерял свои средства ввиду собственной неосмотрительности. Тем не менее, допрос следует произвести надлежащим образом, далее уделить особое внимание другим следственным действиям, позволяющим достоверно установить обстоятельства и факты, имеющие значение для дела (осмотры, обыски, выемки, назначение экспертиз)[71] и, при необходимости, повторно произвести допрос потерпевшего, продемонстрировав собранные доказательства. Как было указано выше, высокий уровень знаний и большой опыт потерпевшего может помочь органам предварительного расследования установить необходимые обстоятельства и факты, однако следователю (дознавателю) необходимо тщательно проверить показания потерпевшего в рамках других следственных действий, чтобы убедиться в их достоверности.

Если потерпевший хранил криптовалюту на кошельке централизованной биржи и сам совершил перевод криптовалюты в адрес злоумышленника, необходимо выяснить:

– с какой целью потерпевшим совершена транзакция, в чей адрес и на каких условиях;

– имелись ли договоренности о переводе криптовалюты в чей-либо адрес взамен на исполнение каких-либо обязательств и исполнены ли обязательства;

– данные о получателе криптовалюты (кроме публичного адреса), если производился обмен криптовалюты через peer-to-peer платформу на

[71] Гайсин Н.И. 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. 294.

национальную валюту (в таких случаях обмен производится между пользователями, верифицированными по паспортным данным или другим документам, содержащим данные о личности).

Если потерпевший хранил криптовалюту на кошельке централизованной биржи и при этом он не совершал перевод криптовалюты в адрес злоумышленника, необходимо выяснить у него:

– какие данные им использовались для регистрации учетной записи;

– наличие или отсутствие у заявителя SIM-карты, с помощью которой осуществлена регистрация на криптовалютных биржах;

– наличие или отсутствие у заявителя доступа к электронной почте, писем на ней о смене пароля учетной записи, если для регистрации учетной записи использовалась электронная почта;

– известно ли ему о том, что третьи лица получали доступ к его SIM-карте или электронной почте, которые использовались для регистрации учетной записи;

– о фактах передачи логина и пароля от электронной почты третьим лицам или по запросам сторонних сайтов, браузерных расширений и децентрализованных приложений;

– восстанавливал ли он доступ к своей учетной записи и причины, по которым пришлось восстанавливать доступ;

– способ хранения пароля от электронной почты;

– использовались ли чужие электронные носители информации для авторизации учетных записей криптовалютных бирж;

– о фактах использования чужих устройств для авторизации учетной записи электронной почты;

– о фактах использования своей SIM-карты на чужих устройствах.

Если потерпевший хранил криптовалюту на некастодиальном кошельке и сам совершил перевод криптовалюты в адрес злоумышленника, необходимо выяснить у него:

– с какой целью потерпевшим совершена транзакция, в чей адрес и на каких условиях;

– имелись ли договоренности о переводе криптовалюты в чей-либо адрес взамен на исполнение каких-либо обязательств и исполнены ли обязательства;

– совершалась ли им покупка активов при помощи децентрализованных приложений по рекомендациям третьих лиц или без таковых;

– наличие или отсутствие переписок с предполагаемым злоумышленником, а также их содержание.

Если потерпевший хранил криптовалюту на некастодиальном кошельке и не переводил криптовалюту в адрес злоумышленника, необходимо выяснить:

– наименование программного обеспечения, приложения, или браузерного расширения, которое использовалось в качестве кошелька, а также источники, откуда они загружены на устройство;

– способ хранения заявителем мнемонической фразы;

– факт передачи заявителем мнемонической фразы третьим лицам или по запросу сайтов, браузерных расширений, децентрализованных приложений;

– наличие или отсутствие транзакций в адрес других кошельков, а также дата, время, сумма, наименование актива и адрес кошелька, на который осуществлен перевод;

– наличие или отсутствие согласий на распоряжение криптовалютными активами децентрализованным приложениям, дата и время их предоставления, а также виды криптовалют, на распоряжение которыми дано согласие, и лимиты, в пределах которых разрешено распоряжение;

– наличие или отсутствие переписок с предполагаемым злоумышленником, а также их содержание.

Благодаря предложенным организационным и тактическим мерам, а также алгоритму действий, сотрудники органов предварительного расследования смогут спланировать и произвести ряд других действий, направленных на установление личности злоумышленника. Однако показания потерпевшего необходимо проверять в ходе других следственных действий, поскольку допрашиваемый может как добросовестно заблуждаться относительно предоставляемой им информации, по разным причинам не упомянуть о важных событиях и фактах, либо намеренно вводить следователя в заблуждение.

3.3. Тактические особенности организации и производства обыска

Проведение обыска на первоначальном этапе расследования хищений криптовалюты необходимо для поиска и изъятия электронных носителей информации, цифровых следов и других доказательств, имеющих значение для дела. Также в рамках этого следственного действия нередко может потребоваться производство ареста криптовалюты.

Данное следственное действие, в большинстве случаев, проводится в местах нахождения, пребывания или проживания подозреваемых (обвиняемых), в отношении самих подозреваемых (личный обыск). Также обыск возможно произвести по месту нахождения криптовалютного обменника, если стало известно, что злоумышленник с его помощью обменял похищенную криптовалюту на национальную валюту.

Для успешного производства 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 рамках подготовки к проведению обыска необходимо привлечь к участию специалиста, обладающего знаниями в сфере информационных технологий, а также имеющего практический опыт работы с криптовалютными сервисами, чье содействие позволит быстро зафиксировать имеющую значение информацию, а также оказать помощь в производстве ареста криптовалюты. Представляется, что при расследовании хищений в сфере оборота криптовалют следователю надлежит заранее наладить контакт с несколькими специалистами соответствующего профиля в целях возможности быстрого обеспечения их присутствия в качестве участника следственного действия, проводимого неотложно. Также данная мера позволит в рамках сотрудничества привлекать одного и того же специалиста к участию в разных следственных действиях или консультированию, что обеспечит осведомленность специалиста о необходимых для его работы обстоятельствах уголовного дела и не потребует потери времени на их разъяснение, позволит быстро сориентироваться при обыске, в каком направлении следует искать требуемую информацию и как проводить ее фиксацию и копирование.[72] Под специалистами соответствующего профиля подразумеваются специалисты, обладающие практическими навыками как в области компьютерных технологий, так и в области криптовалют. Это необходимо для того, чтобы успешно осмотреть, скопировать и изъять необходимую информацию, так и корректно совершить все необходимые действия с криптовалютой.

Существуют разные мнения относительно участия специалиста при изъятии электронного носителя информации. Так, например, по мнению В.Е. Пономарева носители могут изыматься следователем без участия специалиста при условии, что они обнаружены отдельно от иных технических устройств,

[72] Шнейдерова Д.И. Обыск по уголовным делам о хищениях в сфере оборота криптовалют: тактические и процессуальные проблемы // Актуальные проблемы уголовного процесса и криминалистики : сборник научных статей / Министерство внутренних дел Республики Беларусь, учреждение образования «Могилевский институт Министерства внутренних дел Республики Беларусь» ; Могилев : Могилев. институт МВД, 2023. С. 153-154.

либо данные технические устройства находятся в выключенном состоянии.[73] «В случае любых сомнений при изъятии устройств или для их корректного отключения или извлечения полезно привлекать профильных специалистов, ведь неквалифицированные действия создают риск повреждения файлов или уничтожения информации».[74]

Производство обыска целесообразно поручить дознавателю или органу дознания. Однако это не означает, что следователь (дознаватель) не должен находиться по месту производства обыска и следить за ходом следственного действия. Поручение дознавателю или органу дознания произвести обыск, в данном случае, вынужденная тактическая мера, поскольку необходимо предвидеть, что в ходе обыска будут обнаружены криптовалютные кошельки, на балансе которых имеется криптовалюта, и на обнаруженную криптовалюту незамедлительно следует наложить арест, поскольку на практике существуют риски того, что пособники лица, чья криптовалюта подлежит изъятию, могут, получив информацию о задержании владельца кошелька или условный сигнал от последнего, иметь ключи доступа от кошелька хранения криптовалюты и оперативно перевести преступные средства в криптовалюте на другие адреса хранения либо обменять на обычные средства.[75] Если уголовное дело находится в производстве одного следователя (дознавателя), то он будет не в состоянии произвести одновременно два следственных действия, требующих незамедлительности. В связи с изложенным, необходимо заблаговременно получить разрешение суда о наложении ареста на криптовалюту, а также создать криптовалютный кошелек, в адрес которого будет переведена криптовалюта в рамках наложения ареста. Для создания некастодиального

---

[73] Пономарев В.Е. Технико-криминалистическое обеспечение выявления и закрепления электронных доказательств: дис. … к-та юрид. наук: 5.1.4. Москва, 2025. С. 110.

[74] См. например: Пономарев В.Е. Указ. соч. С. 122., Цифровая криминалистика : учебник для вузов / под редакцией В. Б. Вехова, С. В. Зуева. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — С. 36. — (Высшее образование). — ISBN 978-5-534-21152-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/581669 (дата обращения: 17.01.2026).

[75] Осипов Г.П. Указ. соч. 2025. № 3 (107). С. 98.

кошелька, а также консультации по безопасному хранению мнемонической фразы и приватных ключей, во избежание утраты арестованной криптовалюты, следует прибегнуть к помощи специалиста.

Следует отметить, что несмотря на отсутствие законодательно закрепленного порядка ареста криптовалюты, уже существует судебная практика по разрешению наложения ареста на криптовалюту. По данным объединенной пресс-службы городских судов г. Санкт-Петербурга, в апреле 2022 г. районный суд Санкт-Петербурга в рамках уголовного дела, возбужденного по ч. 2 ст. 272 УК РФ, п. «б» ч. 4 ст. 158 УК РФ, разрешил арестовать похищенную криптовалюту ETH, содержащуюся на 24 кошельках обвиняемого в краже и неправомерном доступе к компьютерной информации. Суд пояснил, что по своей сути основным отличием криптоденег от денег является только способ их возникновения, а поскольку понятие криптовалюты не закреплено законодательно, обозначение ее как иного имущества в обвинении, предъявленном фигуранту дела, а также в ходатайстве об аресте допустимо. Криптовалюта используется как средство платежа, инвестиций и накопления сбережений, т.е. имеет материальную ценность, соответственно, признается судом как иное имущество и свидетельствует о наличии предмета преступления по смыслу примечания к ст. 158 УК РФ, на которое может быть наложен арест.[76]

При наложении ареста на криптовалюту может возникнуть проблема, связанная с наличием у обнаруженного кошелька мультиподписи. Ее функция состоит в том, чтобы совершение транзакции было возможно только путем ее утверждения (подписания) несколькими пользователями. В отсутствие достаточного количества подписей, транзакцию, направленную на наложение ареста, совершить не удастся.

В случае если криптовалюта находится на кастодиальном сервисе (например, на централизованной бирже), то аккаунт может быть заморожен на

[76] Осипов Г.П. Указ. соч. 2025. № 3 (107). С. 96.

основании решения суда. Роль специалиста в данном случае заключается в разъяснении следователю и другим участникам процесса о порядке направления запроса на требуемый криптосервис с учетом особенностей его правового статуса, законодательства, регулирующего его деятельность, а также его внутренних политик. Так, специалист по криптовалюте может в такой ситуации подсказать, как направить запрос на криптовалютный сервис от лица правоохранительных органов в случае, если ведомственная почта правоохранительных органов имеет запрет на отправку писем на иностранные сервисы.[77]

Помимо поиска электронных носителей информации, обозначенных выше, следует искать холодные криптовалютные кошельки, которые могут быть как в форме электронных носителей информации, так, например, и в форме пластиковых карт, колец и других предметов, внешне похожих на обычные предметы. Также криптовалютный кошелек может быть в бумажной форме, на которой распечатан QR-код для сканирования, публичный и приватный адрес в виде латинских букв и цифр. Нередко на бумажных носителях хранят мнемонические фразы от кошельков, чтобы исключить взаимодействие с онлайн средой. Помимо криптовалютных кошельков, изъятию в ходе обыска подлежат найденные наличные денежные средства, банковские карты и SIM-карты, так как последние два могли быть использованы для приготовления к совершению хищений путем покупки аккаунтов в различных социальных сетях и мессенджерах, с целью скрыть личность злоумышленника. Банковские карты также могли быть использованы для обналичивания похищенной криптовалюты, а наличные денежные средства также могли быть получены в результате обналичивания похищенной криптовалюты.

Учитывая то, что доступ к криптовалютным кошелькам может быть у нескольких лиц, находящихся в разных местах, возможность дистанционного

[77] Осипов Г.П. Указ. соч. 2025. № 3 (107). С. 93-94.

доступа к электронным носителям информации, а также использование облачных хранилищ, помимо элемента внезапности 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 произвести перевод криптовалюты в адрес другого кошелька, а также перемесить или уничтожить информацию, имеющую значение для дела.

Несмотря на ограничение доступа к связи, 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 ликвидации доступа к сети на изымаемом устройстве, например, включить режим полета, отключить Wi-Fi, GPS, NFC, точки доступа, Bluetooth.[78]

Таким образом, для успешного проведения обыска необходимо принять ряд организационных и тактических мер для недопущения уничтожения следов (в том числе и цифровых), электронных носителей информации и других объектов, имеющих значение для дела, а также перевода похищенной криптовалюты на другой публичный адрес. Также необходима подготовка к наложению ареста на обнаруженную криптовалюту. В ходе проведения обыска необходимо обращать внимание не только на привычные электронные носители информации, но и на наличие холодных криптовалютных кошельков, а также иные объекты материального мира, поскольку они могут иметь значение для дела также, как и электронные носители информации.

[78] Грибунов О.П., Усачев С.И., Усачева Е.А. Указ. соч. С. 7-12.

3.4. Тактика назначения и производства судебных экспертиз при расследовании хищений криптовалюты

Вопросам и проблемам, связанным с назначением и производством экспертиз посвящены работы Т.В. Аверьяновой, Ф.Г. Аминева, О.Г. Дьяконовой, Е.В. Ивановой, Н.П. Майлис, Т.Ф. Моисеевой, Е.Р. Россинской, Г.С. Русман и др.[79]

Назначение экспертиз на первоначальном этапе расследования хищений криптовалюты является одним из важнейших следственных действий, поскольку для установления ряда обстоятельств, имеющих значение для дела, необходимы специальные знания сведущих лиц.

Назначение экспертиз необходимо для решения следующих вопросов:

1. Стоимость криптовалюты на момент хищения.

---

[79] См. например: Аверьянова Т.В. Судебная экспертиза: Курс общей теории. – М.: Норма, 2006. – 480 с., Аминев Ф.Г. Назначение судебных экспертиз: учеб.-методич. Пособие. Уфа: РИЦ БашГУ, 2020. – 159 с., Аминев Ф.Г. Современные проблемы судебно-экспертной деятельности в Российской Федерации и пути их решения: монография. – М.: Юрлитинформ, 2019. – 272 с., Дьяконова О.Г. Специальные знания в судебной и иной юрисдикционной деятельности государств-членов ЕАЭС: теория и практика: дис. … д-ра юрид. наук: 12.00.12. Москва, 2021. 647 с., Иванова Е.В. Концептуальные основы использования специальных знаний при выявлении и расследовании преступлений, связанных с опасными для здоровья веществами: дис. ... д-ра юрид. наук: 12.00.12. Коломна, 2016. 268 с., Моисеева Т.Ф. Классификация судебных экспертиз: необходимость унификации // Вестник экономической безопасности. 2016. № 4. С. 68-72., Россинская Е.Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе: монография. 4-е изд., перераб. и доп. М.: Норма; Инфра-М, 2022. – 576 с., Аминев Ф.Г. О необходимости постоянного совершенствования организационно-правового и методического обеспечения судебно-экспертной деятельности // Вестник Академии правоохранительных органов. 2022. № 4 (26). С. 8-15., Майлис Н.П. О перспективах развития судебной экспертизы в условиях использования современных технологий // Казанские уголовно-процессуальные и криминалистические чтения: материалы II Международной научно-практической конференции (г. Казань, 3 марта 2023 г.): сборник научных статей / члены редакционной коллегии: Н.А. Подольный, И.Г. Гаранина, Ю.Ю. Малышева; ответственный редактор Ю.Н. Кулешов. Казань: Школа, 2023. С. 57-61., Русман Г.С., Бикбаева Э.А. О проблемах осуществления судебно-экспертной деятельности в Челябинской области // Международная научно-практическая конференция «Университетские правовые диалог», посвященная 90-летию со дня рождения профессора, доктора юридических наук, заслуженного деятеля Высшей школы Юрия Даниловича Лившица, Челябинск, 29-30 марта 2019 г.: С. 176-180.

2. Наличие или отсутствие вредоносного программного обеспечения на устройстве, используемом для взаимодействия с похищенной криптовалютой, а также механизм его работы.

3. Наличие или отсутствие вредоносных функций в смарт-контрактах.

4. Получение доступа к изъятым электронным носителям информации, восстановление удаленных цифровых следов и др.

Для ответа на вопрос о стоимости похищенной криптовалюты необходима информация о наименовании похищенной криптовалюты (тикер), его идентификатор (контракт) и количестве похищенных монет или токенов. В случаях, когда транзакция совершена злоумышленником, необходима информация о количестве монет, потраченных для уплаты комиссии майнерам или валидаторам.

Для ответа на второй и четвертый вопрос следует изъять и передать эксперту все электронные носители информации, которые необходимо исследовать на наличие или отсутствие вредоносного программного обеспечения или получить к ним доступ, а также изъять или восстановить удаленные цифровые следы.

Для ответа на третий вопрос необходимо представить на исследование адрес исходного кода децентрализованного приложения, который размещен в блокчейне и общедоступен для всех.

Большинство опрошенных респондентов справедливо считает, что назначение экспертиз по вышеуказанным делам обязательно (приложение 1).

Основными объектами компьютерно-технической экспертизы являются компьютеры, винчестеры, флеш-карты, оптические диски и другие носители информации, сетевые аппаратные средства, цифровые следы, как, например, компьютерная информация, зафиксированная в памяти технических устройств (файлы любого формата, веб-страницы, каталоги, программы и приложения, их исходные коды, операционные системы и их образы, базы данных, протоколы работы системы и отдельных программ, алгоритмы). Среди материальных объектов, кроме компьютеров, можно отметить аппаратные

криптокошельки, среди цифровых – базы данных на блокчейне, программы криптокошельков, криптобирж и обменников, мессенджеров и социальных сетей, электронной почты, браузеров, веб-страницы интернет-ресурсов (в т. ч. кошельков, бирж и обменников, если доступ осуществляется через браузер), лог-файлы программ и иные.[80] К числу перечисленных объектов следует отнести децентрализованные приложения (как их интерфейс, так и исходный код, размещенный на блокчейне).

В отношении объектов, принадлежащих потерпевшему, компьютерно-техническую экспертизу необходимо назначить, если после допроса потерпевшего (получения объяснения от заявителя), изъятия у него электронных носителей информации, осмотра их содержимого появились основания предполагать, что хищение произошло в результате использования злоумышленником вредоносного программного обеспечения.

К постановлению о назначении компьютерно-технической экспертизы следует приложить:

1. Объяснение или протокол допроса потерпевшего, где последний поясняет об обстоятельствах, при которых произошло хищение;

2. Протоколы осмотров электронных носителей информации;

3. Изъятые электронные носители информации.

Данный перечень не является закрытым и при необходимости могут быть представлены другие материалы.

Основные вопросы, которые необходимо поставить перед экспертом:

1. Имеются ли на представленном носителе признаки функционирования вредоносного программного обеспечения?

2. Каков путь расположения файлов, относящихся к вредоносному программному обеспечению?

---

[80] Шнейдерова Д.И. Назначение компьютерно-технической экспертизы по материалам проверки и уголовным делам о хищениях в сфере оборота криптовалют // Правовая культура в современном обществе: Сборник научных статей VI Международной научно-практической конференции, Могилев, 19 мая 2023 года, С. 297.

3. Какую функциональную задачу выполняет обнаруженное вредоносное программное обеспечение?

4. Какую функциональную задачу выполняет представленный на исследование исходный код, размещенный на конкретном блокчейне?

В отношении объектов, принадлежащих подозреваемому, компьютерно-техническую экспертизу необходимо назначить без предварительного осмотра, чтобы исключить риск утери информации и цифровых следов, имеющих значение для дела. В этом случае целесообразно поставить перед сведущими лицами наиболее общие вопросы, подходящие под сложившуюся следственную ситуацию. Полагаем, что тот же подход по постановке вопросов необходимо применять в случае возникновения необходимости в извлечении информации из электронных носителей потерпевшего (или в восстановлении доступа).

Необходимость в назначении экспертизы для определения стоимости похищенной криптовалюты обусловлена тем, что у криптовалюты нет и не может быть официального курса, как у национальной валюты, в силу отсутствия единого регулятора. Также следует отметить, что на сегодняшний день отсутствует единая методика определения стоимости похищенной криптовалюты в рублевом эквиваленте. Нельзя не согласиться с утверждениями О.П. Грибунова, С.И. Усачева и Е.А. Усачевой о том, что на сегодняшний день отсутствует отлаженный механизм определения рублевого эквивалента криптовалюты. Ввиду ее децентрализованного характера тяжело провести судебную товароведческую либо независимую оценочную экспертизу, а проводя их, придется руководствоваться существующими онлайн-конвекторами, работа с которыми также сопряжена с определенными сложностями - в рамках процессуального оформления стоимости имущества становится необходимым устанавливать ее реальный размер на момент хищения, для чего следует знать время совершения преступления, а также придется учитывать тот факт, что различные криптобиржи указывают разную

стоимость криптовалюты, а это в конечном итоге может повлиять и на квалификацию деяния.[81]

На наш взгляд, при определении стоимости похищенной криптовалюты существует ряд проблем. Начать следует с проблемы, которая выражается в том, что, в подавляющем большинстве случаев, рыночная и покупная стоимости криптовалюты в рублевом эквиваленте могут существенно отличаться. Это связано с высокой волатильностью курсов криптовалют к доллару США, изменчивостью курса доллара США к рублю, а также наличием различных способов покупки и продажи криптовалюты. Так, например, в конкретную дату и время рыночная стоимость криптовалюты BTC может быть равна 100 000 долларов США за 1 BTC, а 1 доллар США по курсу ЦБ РФ может быть равен 80 рублям. В этом случае рыночная стоимость 0,0005 BTC в рублевом эквиваленте равна 4000 рублей. На момент хищения курс BTC может снизиться до 70 000 долларов США, а курс 1 доллара США снизиться до 70 рублей. В таком случае следует вывод, что на момент совершения хищения стоимость похищенной криптовалюты в рублевом эквиваленте равна 2 450 рублям. Тот факт, что рыночная стоимость 0,0005 BTC в рублевом эквиваленте равна 4000 рублей на момент покупки, не означает, что покупная стоимость тоже равна 4000 рублям, так как, в большинстве случаев, покупка криптовалюты осуществляется через peer-to-peer платформу и обменники, которые продают криптовалюту по более высокому курсу. Каждый продавец криптовалюты устанавливает собственный курс, по которому готов купить или продать криптовалюту. Поэтому покупная цена будет зависеть от конкретного выбора покупателя.

Исходя из вышеизложенного, считаем, что при определении стоимости похищенной криптовалюты исходить из покупной стоимости некорректно, так

[81] Грибунов О.П., Усачев С.И., Усачева Е.А. Криптовалюта и иные виртуальные активы как феномен современной преступности: проблемы раскрытия, расследования и предупреждения // Российский следователь. 2024. № 4. С. 7-12. [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 14.06.2025).

как по истечении определенного количества времени, ввиду высокой волатильности, рыночная стоимость криптовалюты может существенно отличаться от покупной. Исходить следует из рыночной стоимости криптовалюты на момент совершения хищения.

Следующая проблема заключается в том, что цены на одну и ту же криптовалюту в одно и то же время на разных криптовалютных биржах отличаются. Так, например, в определенную дату и время стоимость ETH на криптовалютной бирже «Binance» может быть 4 000 долларов США. В то же время ETH на криптовалютной бирже «OKX» может стоить 3 990 долларов США, а на криптовалютной бирже «Bybit» - 4 005 долларов США.

Принцип правовой определенности и толкования всех неустранимых сомнений в пользу обвиняемого предопределяет следующее предложение. Во-первых, проводится экспертиза, которая устанавливает курс криптовалюты за период, в который совершалось преступное изъятие. Во-вторых, по делам, в которых отсутствовала воля потерпевшего на передачу криптовалюты за какую-либо стоимость, эксперт предоставляет сведения о максимальном и минимальном биржевом курсе (с разных бирж) на момент совершения преступления или в период, когда совершались деяния. Если же установлена воля потерпевшего на определенную сумму (и согласие на эту стоимость не было сформировано под влиянием обмана), то в данную «вилку» включается и она. А далее, следуя презумпции, суд рассматривает в качестве причиненного ущерба наименьший из показателей, приведенных в заключении эксперта за конкретный период.[82]

Однако существует криптовалюта, которая не размещена на централизованных криптовалютных биржах, но имеет ценность. Часто такая криптовалюта не подлежит обмену на национальную валюту, поскольку у обменников и peer-to-peer мерчантов нет спроса на эту криптовалюту. Однако вышеуказанная криптовалюта размещена на децентрализованных биржах и

[82] Филатова М.А. Проблемы установления размера и ущерба при квалификации посягательства на цифровую валюту // Уголовное право. 2022. № 1/2022. С. 71.

также может стоить по-разному на разных децентрализованных биржах. Поэтому такую криптовалюту возможно обменять на криптовалюту, которую, в свою очередь, возможно продать в обмен на национальную валюту. В связи с изложенным, считаем возможным определить стоимость неразмещенной на централизованных биржах похищенной криптовалюты аналогично тому, как определяется рыночная стоимость размещенных на централизованных биржах криптовалют.

Такой же подход считаем наиболее рациональным и при оценке стоимости похищенной NFT, с некоторыми особенностями. Следует отметить, что такая криптовалюта размещается и торгуется на децентрализованных приложениях, являющихся NFT маркетплейсами. Такой токен торгуется за определенное количество конкретной криптовалюты. NFT на маркетплейсах имеет две цены. Первая определяется лицом, разместившим NFT, вторая определяется исходя из спроса и предложения и называется флор прайс. Владелец NFT может определить стоимость своего токена ниже, выше или на уровне флор прайса. Так, например, собственник какой-либо NFT мог разместить ее и выставить цену в количестве 10 ETH при флор прайсе 0,001 ETH. Однако при оценке стоимости похищенного токена следует исходить из рыночной стоимости того количества криптовалюты, за которое собственник имел реальную возможность продать свой токен в момент хищения.

Также следует отметить несколько особенностей, вытекающих из специфики технологии блокчейн и криптовалютной индустрии. При совершении хищения потерпевшему всегда причиняется ущерб, превышающий рыночную стоимость выведенной из кошелька потерпевшего криптовалюты, поскольку за совершение транзакций необходима уплата комиссий блокчейна, предназначающихся майнерам или валидаторам (в некоторых случаях для совершения хищения может потребоваться совершение не одной, а нескольких транзакций), а также комиссий, предназначающихся криптовалютной бирже (если транзакции осуществлены с кастодиального кошелька), децентрализованному приложению (если транзакции совершены с

некастодиального кошелька и перед совершением хищения злоумышленник совершил транзакцию по изъятию криптовалюты, размещенной в децентрализованном приложении). Уплату комиссий при совершении транзакции злоумышленником также следует квалифицировать в качестве хищения исходя из положений УК РФ о хищении. Если же криптовалюта была переведена в адрес злоумышленника самим потерпевшим, полагаем, что уплаченную комиссию за перевод не следует включать в сумму похищенного.

Для назначения экспертизы, с целью определения стоимости похищенной криптовалюты, необходимо полное и корректное изложение обстоятельств и фактов для сведущего лица, а также постановка правильных вопросов.

В постановлении о назначении экспертизы, помимо прочего, необходимо указать наименование похищенной криптовалюты (тикер) с идентификатором (контракт), дату и период времени, в который совершено хищение, начиная с момента совершения транзакции, направленной на хищение, и заканчивая моментом поступления криптовалюты в адрес злоумышленника. Если хищение совершено с кастодиального кошелька, необходимо указать, какой криптовалютной бирже принадлежит данный кошелек. Если совершено хищение криптовалюты, размещенной на децентрализованном приложении, необходимо указать наименование и URL адрес этого децентрализованного приложения.

К постановлению о назначении экономической экспертизы следует приложить:

1. Объяснение или протокол допроса потерпевшего;

2. Протоколы осмотров электронных носителей информации, в которых объектами осмотров были транзакции, отображенные в блокчейн-обозревателях и (или) криптовалютных кошельках, в результате совершения которых произошло хищение;

3. Протоколы осмотров электронных носителей информации, в которых объектами осмотров были банковские приложения, платежные документы,

истории сообщений в мессенджерах, электронных почтах и других сервисах, подтверждающих покупку потерпевшим криптовалюты.

Данный перечень не является закрытым и при необходимости могут быть представлены другие материалы.

Перед экспертом-экономистом необходимо поставить следующие вопросы:

1. Какова наименьшая рыночная стоимость конкретного количества криптовалюты на конкретном блокчейне на момент совершения хищения?

2. При отсутствии возможности продажи конкретной криптовалюты на конкретном блокчейне за фиатную валюту, возможно ли совершить сделку по обмену данной криптовалюты на ту криптовалюту, в отношении которой на момент совершения хищения было возможно совершить сделку по ее продаже за фиатную валюту?

3. Какова на момент хищения наименьшая рыночная стоимость конкретной криптовалюты на конкретном блокчейне, уплаченной в качестве комиссий на конкретных площадках (биржах и децентрализованных приложениях) для осуществления хищения?

В случаях, когда нет возможности установить адреса и ID транзакции, чтобы начать осмотр блокчейн-обозревателя, нет доступа к криптовалютному кошельку потерпевшего, поскольку, например, отсутствует доступ к электронным носителям информации, необходима комплексная компьютерно-техническая и экономическая экспертиза, когда сначала необходимо установить технические подробности события хищения, а затем дать его экономическую характеристику.[83]

Иногда невозможно определить вредоносность децентрализованного приложения экспертным путем как ввиду отсутствия необходимого уровня компетенций сведущих лиц или отсутствием сведущих лиц, так и ввиду

[83] Виноградова М.М. Возможности судебной экономической экспертизы при расследовании преступлений, связанных с оборотом криптовалюты // Российский следователь. 2024. № 8. С. 2-5.

закрытого исходного кода децентрализованного приложения, в силу чего недоступен предмет исследования. Следует пояснить, что программный код децентрализованных приложений размещается на блокчейне. Этот код может быть открытым и в этом случае его содержание может изучить любой желающий, а может быть закрытым и в этом случае указать на необходимый исходный код сведущему лицу для проведения экспертизы не представится возможным.

Проверить децентрализованное приложение с закрытым исходным кодом возможно путем проведения следственного эксперимента. Перед проведением следственного эксперимента необходимо в ходе осмотра установить, какое децентрализованное приложение совершило вывод криптовалюты из кошелька потерпевшего и предоставлялось ли ему разрешение на распоряжение криптовалютой. К проведению следственного действия целесообразно привлечь специалиста, обладающего практическим опытом во взаимодействии с криптовалютой и децентрализованными приложениями, а также обладающего умением правильно интерпретировать транзакции в блокчейн-обозревателе. Далее необходимо создать некастодиальный криптовалютный кошелек и внести в его адрес ту же криптовалюту на том же блокчейне, что была похищена у потерпевшего. Если эта криптовалюта не является основной монетой в блокчейне, необходимо внести в адрес созданного кошелька криптовалюту, являющуюся основной монетой блокчейна. В противном случае, совершить какие-либо транзакции в рамках следственного эксперимента не представится возможным. После пополнения баланса криптовалютного кошелька необходимо подключить его к проверяемому децентрализованному приложению, а далее совершить все действия, которые совершил потерпевший, исходя из информации, отображенной в ранее осмотренном блокчейн-обозревателе. Если сразу после произведенных действий не произойдет каких-либо списаний, следует приостановить следственный эксперимент и продолжить его после того, как будет обнаружен вывод средств из кошелька. Далее необходимо зафиксировать

наличие транзакции по выводу средств в блокчейн-обозревателе, после чего следует завершить производство следственного эксперимента.

Все произведенные действия в рамках следственного эксперимента следует зафиксировать путем фото и видеосъемки. В частности, необходимо зафиксировать публичный адрес криптовалютного кошелька, откуда ожидается совершение нового хищения, и баланс кошелька, как после пополнения, так и после вывода средств.

В протоколе следственного эксперимента необходимо зафиксировать каждое произведенное действие, начиная с момента создания некастодиального кошелька с указанием публичного адреса или публичных адресов, которые необходимо пополнить, и завершая моментом открытия вредоносной транзакции в блокчейн-обозревателе, указав публичные адреса кошельков, откуда была выведена криптовалюта и куда направлена.

ЗАКЛЮЧЕНИЕ

Проведенное комплексное исследование теоретических и практических проблем расследования дистанционных хищений криптовалютных активов позволило сделать следующие выводы.

1. Для эффективного расследования дистанционных хищений криптовалюты следователям (дознавателям) необходимо обладать знаниями понятийного аппарата криптовалютной экосистемы, а также знаниями об особенностях взаимодействия с технологией блокчейн и криптовалютой.

2. Вне зависимости от конкретного способа (схемы) дистанционного хищения криптовалюты:

– любое дистанционное хищение криптовалюты происходит в результате использования злоумышленником входных данных (мнемонической фразы, приватного ключа, логина и пароля), позволяющих получить доступ к криптовалютному кошельку (биржевому аккаунту), либо предоставления разрешения вредоносному децентрализованному приложению распоряжаться криптовалютой, либо в результате перевода криптовалюты потерпевшим в адрес злоумышленника.

3. Криптовалюта является предметом преступного посягательства также, как наличные и безналичные денежные средства, а также иное имущество, имеющее ценность.

4. Основными элементами криминалистической характеристики дистанционного хищения криптовалюты являются предмет хищения, способ совершения хищения и сокрытия следов хищения, следообразование в виде электронных (цифровых) следов, личность преступника, а также личность потерпевшего.

5. Для возбуждения уголовного дела по факту дистанционного хищения криптовалюты в результате перевода криптовалюты потерпевшим в адрес злоумышленника достаточно получить объяснение от заявителя, в котором он утверждает о личной инициации транзакции в адрес злоумышленника;

произвести осмотр электронного носителя информации, а именно, истории транзакции криптовалютного кошелька и блокчейн-обозревателя для подтверждения наличия транзакции; произвести осмотр электронного носителя информации, а именно, той информации, которая указывает на то, что транзакция совершена под воздействием обмана или в результате злоупотребления доверием.

Для возбуждения уголовного дела по факту дистанционного хищения криптовалюты в результате использования злоумышленником входных данных (мнемонической фразы, приватного ключа, логина и пароля), позволяющих получить доступ к криптовалютному кошельку (биржевому аккаунту), либо предоставления разрешения вредоносному децентрализованному приложению распоряжаться криптовалютой, достаточно получить объяснение от заявителя, в котором он утверждает об инициации транзакции третьими лицами; произвести осмотр электронного носителя информации, а именно, истории транзакции криптовалютного кошелька и блокчейн-обозревателя для подтверждения наличия транзакций; произвести действия, направленные на подтверждение того, что в адрес третьих лиц была передана информация, обеспечивающая доступ к криптовалюте, либо было дано разрешение вредоносному децентрализованному приложению распоряжаться криптовалютой.

6. Первоначальный этап расследования дистанционных хищений криптовалюты характеризуется открытым характером информации об объективных признаках совершенного преступления и дефицитом информации о лице, совершившем хищение.

7. Следственная ситуация, в большинстве случаев, редко может быть благоприятной ввиду дистанционного характера хищения, отсутствия привязки криптовалютных кошельков к личности, а также использования злоумышленником способов сокрытия следов хищения (использование анонимных блокчейнов, VPN сервисов, подставных лиц и т.д.).

8. Выдвижение типичных следственных версий следует начать с выяснения обстоятельств, при которых совершена транзакция, повлекшая хищение (совершил ли транзакцию сам потерпевший или же злоумышленник), а также с выяснения способа хранения криптовалюты. Знание ответов на эти два вопроса позволит выдвинуть более продвинутые версии и проверить их. При этом следует проверить версию о добросовестном заблуждении относительно совершения хищения.

9. Взаимодействие с органами, осуществляющими оперативно-розыскную деятельность, должно осуществляться для установления личности злоумышленника и его поиска, а также помощи в производстве отдельных следственных действий.

10. Существует ряд проблем организационного, технического, и процессуального характера, препятствующих эффективному взаимодействию с оперативно-розыскными органами для расследования хищений криптовалюты, среди которых основными считаем: отсутствие достаточных знаний у сотрудников оперативных подразделений о криптовалюте; ограниченное количество компетентных экспертов и специалистов в области компьютерно-технических экспертиз; отсутствие эффективного международного сотрудничества в части обмена информацией.

11. Получение объяснения от заявителя, а далее допрос потерпевшего – первое, с чего необходимо начать расследование хищений криптовалюты, поскольку полученная информация может помочь сузить круг поиска информации в блокчейн-обозревателях и криптовалютных кошельках. Начинать необходимо с вопросов, касающихся способа хранения криптовалюты и инициатора транзакции, в результате совершения которой совершено хищение. Полученная информация должна быть проверена в ходе других следственных действий.

12. Осмотр криптовалютных кошельков и блокчейн-обозревателей с помощью электронных носителей информации – единственный способ, позволяющий объективно установить наличие транзакции, повлекшей

дистанционное хищение, а также некоторые необходимые для предварительного расследования объективные признаки (время, количество и наименование похищенной криптовалюты, адреса кошелька-отправителя и кошелька-получателя). Осмотр остальных электронных (цифровых) следов второстепенен. Полученная в рамках таких осмотров информация должна дополнять информацию, полученную в рамках осмотров криптовалютных кошельков и блокчейн-обозревателей. При наличии возможности, осмотр криптовалютных кошельков, блокчейн-обозревателей и других электронных ресурсов следует произвести сразу после допроса (получения объяснения). В отсутствие такой возможности необходимо произвести осмотр перечисленных объектов и изъятие электронных носителей информации по месту жительства потерпевшего (заявителя).

13. Для расследования хищений криптовалюты необходимо назначение и проведение экономической экспертизы для определения стоимости похищенного.

14. Назначение и проведение компьютерно-технической экспертизы необходимо для изъятия информации из электронных носителей, принадлежащих подозреваемому; восстановления удаленной информации; восстановления доступа к электронному носителю и информации, содержащейся на нем; а также при выдвижении версии о хищении криптовалюты в результате получения доступа к криптовалютному кошельку и наличия оснований полагать, что для доступа к кошельку и (или) совершения хищения использовано вредоносное программное обеспечение.

15. Рублевая стоимость похищенной криптовалюты определяется исходя из курса доллара США и наименьшей рыночной стоимости криптовалюты на момент хищения в силу законодательных положений о презумпции невиновности. Если незаконную транзакцию совершает злоумышленник, подлежит учету рублевая стоимость комиссии, потраченной для совершения хищения.

16. Успешное проведение обыска обусловлено принятием ряда организационных и тактических мер для недопущения уничтожения следов (в том числе и цифровых), электронных носителей информации и других объектов, имеющих значение для дела, а также перевода похищенной криптовалюты на другой публичный адрес. В ходе проведения обыска необходимо обращать внимание не только на привычные электронные носители информации, но и на наличие холодных криптовалютных кошельков, а также на иные объекты материального мира, поскольку они могут иметь значение для дела также, как и электронные носители информации и электронные (цифровые) следы. Во время проведения обыска необходимо быть готовым к наложению ареста на обнаруженную криптовалюту до ее перевода сообщниками подозреваемого на другой публичный адрес.

17. Для производства всех необходимых следственных действий в рамках расследования дистанционных хищений криптовалюты необходимо взаимодействие с лицами, обладающими специальными знаниями.

СПИСОК ЛИТЕРАТУРЫ

Нормативно-правовые акты и иные официальные документы

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 04.12.2025).

2. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 04.12.2025).

3. Налоговый кодекс Российской Федерации (часть первая) от 31.07.1998 № 146-ФЗ [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 04.12.2025).

4. Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 04.12.2025).

5. Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 04.12.2025).

6. Федеральный закон от 29.11.2024 № 418-ФЗ «О внесении изменений в части первую и вторую Налогового кодекса Российской Федерации и отдельные законодательные акты Российской Федерации» [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 14.11.2025).

Судебная и следственная практика

7. Постановление Пленума Верховного Суда РФ от 27 декабря 2002 г. № 29 «О судебной практике по делам о краже, грабеже и разбое»

[Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 04.12.2025).

8. Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 04.12.2025).

9. Кассационное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 15.11.2023 № 88-УДП23-7-К8 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 27.09.2025).

10. Определение Третьего кассационного суда общей юрисдикции от 24.06.2021 № 77-1411/2021 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 27.09.2025).

11. Кассационное определение Восьмого кассационного суда общей юрисдикции от 21.12.2023 № 77-5316/2023 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 27.09.2025).

12. Определение Первого кассационного суда общей юрисдикции от 20.08.2025 № 77-2652/2025 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 27.09.2025).

13. Апелляционное определение Санкт-Петербургского городского суда от 23.11.2020 № 22-5295/2020, 1-95/2020 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 01.06.2025).

14. Апелляционное определение Московского городского суда от 03.02.2025 по делу № 10-1253/2025 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 01.07.2025).

15. Апелляционное определение Московского областного суда от 16.09.2025 по делу № 22-8217/2025 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 01.07.2025).

16. Апелляционное определение Московского городского суда от 14.10.2025 по делу № 10-19905/2025 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 14.11.2025).

17. Приговор Октябрьского районного суда города Тамбова от 15.02.2019 № 1-134/19 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 01.07.2025).

18. Приговор Зеленоградского районного суда города Москвы от 24.05.2022 по делу № 1-93/2022 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 01.07.2025).

19. Приговор Самарского гарнизонного военного суда от 18.11.2022 № 1-67/2022 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 14.06.2025).

20. Приговор Дорогомиловского районного суда города Москвы от 20.06.2023 по делу № 1-85/2023 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 01.07.2025).

21. Приговор Дорогомиловского районного суда города Москвы от 27.11.2023 по делу № 1-645/2023 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 14.06.2025).

22. Приговор Дорогомиловского районного суда города Москвы от 10.04.2024 по делу № 1-34/2024 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 15.08.2024).

23. Приговор Первомайского районного суда города Краснодара от 17.04.2024 по делу № 1-212/2024 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 14.06.2025).

24. Приговор Тимирязевского районного суда города Москвы от 17.09.2024 по делу № 1-320/2024 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 14.06.2025).

25. Приговор Новгородского районного суда Новгородской области от 18.11.2024 № 1-947/2024 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 14.06.2025).

26. Приговор Октябрьского районного суда города Ижевска от 26.11.2024 по делу № 1-318/2024 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 14.06.2025).

27. Приговор Дорогомиловского районного суда города Москвы от 25.12.2024 № 01-0276/2024 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 01.07.2025).

28. Уголовное дело № 12401270015001224 СУ МВД России по г. Уфе.

Учебники, монографии, учебные пособия

29. Аверьянова Т.В. Судебная экспертиза: Курс общей теории. – М.: Норма, 2006. – 480 с.

30. Аминев Ф.Г. Назначение судебных экспертиз: учеб.-методич. Пособие. Уфа: РИЦ БашГУ, 2020. – 159 с.

31. Аминев Ф.Г. Современные проблемы судебно-экспертной деятельности в Российской Федерации и пути их решения: монография. – М.: Юрлитинформ, 2019. – 272 с.

32. Арцишевский Г.В. Выдвижение и проверка следственных версий. М.: Юрид. лит., 1978. С. 53.

33. Баев О.Я. Основы криминалистики: курс лекций. М.: Экзамен, 2001. 288 с.

34. Белкин Р.С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики / Р. С. Белкин. — М.: Издательство НОРМА (Издательская группа НОРМА–ИНФРА М), 2001. 237 с.

35. Белкин Р.С. Криминалистика: проблемы, тенденции, перспективы. – М.: Юрид. лит., 1988. – 302 с.

36. Белкин Р.С., Винберг А.И., Дорохов В.Я. и др. Теория доказывания в советском уголовном праве. М.: Юрид. лит., 1973. С. 342.

37. Бертовский Л.В. Технология блокчейна в уголовном процессе как элемент цифрового судопроизводства // Проблемы экономики и юридической практики. 2017. № 6. С. 226-230.

38. Бессонов А.А. Основы криминалистического учения об исследовании и использовании криминалистической характеристики преступлений. М.: Юрлитинформ, 2016. С. 256 с.

39. Варданян А.В., Плясов К.А. Оперативно-розыскное обеспечение предупреждения, раскрытия и расследования преступлений в сфере внешнеэкономической деятельности // Юристъ Правоведъ. 2022. № 1 (100). С. 94-99.

40. Васильев А.Н., Н.П. Яблоков. Предмет, система и теоретические основы криминалистики. – Москва, 1984. – 118 с.

41. Россинская Е.Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе: монография. 4-е изд., перераб. и доп. М.: Норма; Инфра-М, 2022. – 576 с.

42. Цифровая криминалистика : учебник для вузов / под редакцией В. Б. Вехова, С. В. Зуева. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 485 с. — (Высшее образование). — ISBN 978-5-534-21152-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/581669 (дата обращения: 17.01.2026).

43. Халиков, А. Н. Оперативно-розыскная деятельность : учебник – 3-е изд. – Москва : РИОР : ИНФРА-М, 2024. – 331 с.

44. Эксархопуло А.А., Макаренко И.А., Зайнуллин Р.И. Криминалистика : учебник для вузов - Москва : Издательство Юрайт, 2025. - 477 с.

45. Яблоков Н.П. Криминалистика: учеб. М., 2000. 371 с.

46. Аминев Ф.Г. О необходимости постоянного совершенствования организационно-правового и методического обеспечения судебно-экспертной деятельности // Вестник Академии правоохранительных органов. 2022. № 4 (26). С. 8-15.

47. Безручко Е.В., Ходусов А.А. Преступления, совершаемые с использованием информационно-коммуникационных средств: философско-правовое конструирование эффективных классификаций // Философия права. 2020. № 3 (94). С. 89-95 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 10.11.2025).

48. Былинкина Е.В. Блокчейн: правовое регулирование и стандартизация // Право и политика. 2020. № 9. С. 143-155. [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 12.08.2024).

49. Вайпан В.А. Основы правового регулирования цифровой экономики // Право и экономика. 2017. № 11. С. 5-18. [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 11.09.2024).

50. Варданян А.В. Проблема систематизации цифровых методов оперативно-розыскной деятельности, используемых в борьбе с дистанционными хищениями, и их криминалистическое значение // Юрист-Правоведъ. 2022. № 2 (101). С. 7-13.

51. Виноградова М.М. Возможности судебной экономической экспертизы при расследовании преступлений, связанных с оборотом криптовалюты // Российский следователь. 2024. № 8. С. 2-5.

52. Вяткин, А. Н. ОРД против киберпреступности: обеспечена ли оперативность? / А. Н. Вяткин // Высокотехнологичное право: современные вызовы: Материалы IV Международной межвузовской научно-практической конференции, Москва-Красноярск, 17–20 февраля 2023 года. Том Часть 2. –

Красноярск: Красноярский государственный аграрный университет, 2023. – С. 29-33.

53. Вяткин, А. Н. Предложения по изменению законодательства для повышения эффективности оперативно-разыскной деятельности в борьбе с киберпреступностью / А. Н. Вяткин // Криминалистическая тактика: история, современное состояние и перспективы развития (к 85-летию со дня рождения профессора В. И. Комиссарова): материалы Международной научно-практической конференции, Москва, 14 марта 2024 года. – Москва: Проспект, 2024. – С. 51-54.

54. Вяткин, А. Н. Проблемы противодействия киберхищениям и пути их решения / А. Н. Вяткин // Право и инновации: новые вызовы технологической революции: Материалы II Приволжского юридического конгресса, Уфа, 21 октября 2022 года. – Уфа: Научно-исследовательский институт проблем правового государства, 2022. – С. 36-44.

55. Гавло В.К. Следственная ситуация // Следственная ситуация: Сб. науч. тр. – М.: Всесоюз. ин-т по изучению причин и разработке мер предупреждения преступности, 1984.

56. Гаврилин Ю.В., Бедеров И.С. Установление личности владельцев цифровой валюты: методологические основы // Труды Академии управления МВД России. 2021. № 4(60). С. 101-108.

57. Гайсин Н.И. 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.

58. Гайсин Н.И. К вопросу о необходимости криминалистического обеспечения расследования хищений криптовалютных активов // Вестник Института права Башкирского государственного университета. 2024. № 4(24). С. 160.

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

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

61. Гейкина И.В. Понятия цифровой валюты и криптовалюты, их отличия // Нотариальный вестник. 2023. № 7. С. 17-23. [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 10.11.2025).

62. Герасимов И.Ф. К вопросу о следственной ситуации // Следственная ситуация: Сб. науч. тр. – М.: Всесоюз. ин-т по изучению причин и разработке мер предупреждения преступности, 1984.

63. Грибунов О.П., Усачев С.И., Усачева Е.А. Криптовалюта и иные виртуальные активы как феномен современной преступности: проблемы раскрытия, расследования и предупреждения // Российский следователь. 2024. № 4. С. 7-12. [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 14.06.2025).

64. Ефимова Л.Г., Сиземова О.Б. Правовая природа смарт-контракта // Банковское право. 2019. № 1. С. 23-30. [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 10.06.2025).

65. Зенин С.С., Кутейников Д.Л., Ижаев О.А., Япрынцев И.М. Правотворчество в условиях алгоритмизации права // Lex russica. 2020. № 7 (164). С. 97-104. [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 10.06.2025).

66. Ишин И.А. Особенности производства отдельных следственных действий и роль начальника органа дознания при расследовании преступлений, совершенных с использованием криптовалют // Сетевое издание «Академическая мысль». 2020. № 2 (11). С. 82-85.

67. Казова З.М., Иванов З.А., Татаров Т.К., Шабатуков И.А., Шугушхов С.З. Цифровые экосистемы // Инновационная экономика: информация, аналитика, прогнозы. 2024. № 2. С. 123-129.

68. Каневский Л.Л. Криминалистическая характеристика преступления, криминальные и следственные ситуации и их значение в раскрытии и расследовании преступлений несовершеннолетних // Вопросы совершенствования борьбы с преступностью несовершеннолетних. – Уфа: Изд-во БашГУ, 1983. – С. 71-82.

69. Каневский Л.Л. Разработка типовых криминалистических характеристик преступлений и их использование в процессе расследования // Российский юридический журнал. 2000. № 2. С. 101-111.

70. Комаров И.М., Пономаренко Н.Ю., Ян Е.И. Ситуационный подход как научно-практическая категория криминалистики // Сибирские уголовно-процессуальные и криминалистические чтения. 2017. № 3 (17). С. 104-115.

71. Коновалова В.Е., Колесниченко А.Н. Теоретические проблемы криминалистической характеристики // Криминалистическая характеристика преступлений: сб. науч. тр. – М., 1984.

72. Майлис Н.П. О перспективах развития судебной экспертизы в условиях использования современных технологий // Казанские уголовно-процессуальные и криминалистические чтения: материалы II Международной научно-практической конференции (г. Казань, 3 марта 2023 г.): сборник научных статей / члены редакционной коллегии: Н.А. Подольный, И.Г. Гаранина, Ю.Ю. Малышева; ответственный редактор Ю.Н. Кулешов. Казань: Школа, 2023. С. 57-61.

73. Макаренко И.А., Эксархопуло А.А. Сущность и правовые формы поисковой деятельности следователя // Философия права. 2024. № 4 (111). С. 149.

74. Мельник Л.Л. Подготовительный этап допроса подозреваемого при расследовании преступлений против собственности, совершенных с

использованием криптовалют и электронных денег / Л.Л. Мельник // Сацыяльна-эканамічныя і прававыя даследаванні. 2023. № 1(71). С. 75-81.

75. Моисеева Т.Ф. Классификация судебных экспертиз: необходимость унификации // Вестник экономической безопасности. 2016. № 4. С. 68-72.

76. Осипов Г.П. Изъятие и арест криптовалюты: роль и участие специалиста // Вестник Университета прокуратуры Российской Федерации. 2025. № 3 (107). С. 93-100.

77. Перов В.А. О криминалистической методике выявления преступлений, совершаемых с использованием криптовалюты, и расследовании соответствующих уголовных дел // Российский следователь. 2020. № 12. С. 10-13. [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 14.06.2025).

78. Родикова В.А. Блокчейн-технологии и персональные данные граждан: перспективы правового регулирования // Российская юстиция. 2023. № 5. С. 72-80. [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 10.05.2024).

79. Рощупкина А.В. Специфика криптовалют для целей оперативно-розыскной деятельности // Вестник Удмуртского университета. 2025. № 3(35). С. 526-532.

80. Руденко А.В. Мыслительная деятельность следователя (дознавателя) при поиске следов преступления // Юридический вестник Кубанского государственного университета. 2015. № 1 (22). С. 18-21.

81. Русман Г.С., Бикбаева Э.А. О проблемах осуществления судебно-экспертной деятельности в Челябинской области // Международная научно-практическая конференция «Университетские правовые диалог», посвященная 90-летию со дня рождения профессора, доктора юридических наук, заслуженного деятеля Высшей школы Юрия Даниловича Лившица, Челябинск, 29-30 марта 2019 г.: С. 176-180.

82. Савельев А.И. Некоторые правовые аспекты использования смарт-контрактов и блокчейн-технологий по российскому праву // Закон. 2017. № 5. С. 94-117. [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 14.06.2024).

83. Тисен О.Н. Методика обнаружения, фиксации и изъятия электронно-цифровых следов по делам о преступлениях, совершенных с использованием криптовалют // Уголовное право. 2024. № 3. С. 69-80. [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 14.06.2025).

84. Тисен О.Н. Специфика расследования преступлений, совершенных с использованием криптовалют // Новые, появляющиеся и видоизменяющиеся формы преступности: научные основы противодействия (Долговские чтения): сб. материалов II Всерос. науч.-практ., Москва, 24-25 марта 2022 г.: С. 333-346.

85. Титов А.А. Отдельные особенности рассмотрения сообщений (заявлений) о преступлениях, совершенных с использованием криптовалют // Вестник Академии Следственного комитета Российской Федерации. 2023. № 2(36). С. 123.

86. Фарахиев Д.М. Деятельность органов внутренних дел в процессе раскрытия и расследования преступлений, совершаемых с использованием информационно-коммуникационных технологий (на примере криптовалютных активов) // Юридический вестник Самарского университета. 2023. № 3(9). С. 81-90.

87. Филатова М.А. Проблемы установления размера и ущерба при квалификации посягательства на цифровую валюту // Уголовное право. 2022. № 1/2022. С. 65-72.

88. Хайдаров А.А. Установление владельца адреса криптокошелька в практике правоохранительных органов // Российский следователь. 2024. № 8. С. 39-42. [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 14.06.2025).

89. Харина Е.А. К вопросу о криминалистической характеристике мошенничества в сфере компьютерной информации // Российский следователь. 2023. № 11. С. 11-15. [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 14.06.2025).

90. Чихрадзе А.М. Семантика криптовалютной экосистемы: вызовы для криминалистической терминологии // Российский следователь. 2025. № 6. С. 14-18. [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 10.11.2025).

91. Шнейдерова Д.И. Использование специальных знаний при расследовании хищений в сфере оборота криптовалют // Вестник криминалистики. 2020. № 4(76). С. 101-107.

92. Шнейдерова Д.И. Назначение компьютерно-технической экспертизы по материалам проверки и уголовным делам о хищениях в сфере оборота криптовалют // Правовая культура в современном обществе: Сборник научных статей VI Международной научно-практической конференции, Могилев, 19 мая 2023 года, С. 296-301.

93. Шнейдерова Д.И. Обыск по уголовным делам о хищениях в сфере оборота криптовалют: тактические и процессуальные проблемы // Актуальные проблемы уголовного процесса и криминалистики : сборник научных статей / Министерство внутренних дел Республики Беларусь, учреждение образования «Могилевский институт Министерства внутренних дел Республики Беларусь» ; Могилев : Могилев. институт МВД, 2023. С. 153-158.

94. Шнейдерова Д.И. Осмотр онлайн-криптокошелька заявителя/потерпевшего (по материалам и уголовным делам о хищениях в сфере оборота криптовалют): процессуальный и криминалистический аспекты // Алтайский юридический вестник № 4 (40) 2022 г. С. 156-162.

95. Шнейдерова Д.И. Особенности криминалистической характеристики личности потерпевшего по делам о хищениях в сфере оборота криптовалют // Актуальные вопросы права, образования и психологии. 2021. Т 9. С. 148-154.

96. Шнейдерова Д.И. Тактические особенности допроса подозреваемого по делам о хищениях в сфере оборота криптовалют // Борьба с преступность: теория и практика: материалы докладов XI Международной научно-практической конференции, Могилев, 07 апреля 2023 г.: С. 490-493.

97. Шнейдерова Д.И. Типичные следственные ситуации по материалам проверки и уголовным делам о хищениях в сфере оборота криптовалют // Концептуальные основы современный криминалистики: теория и практика: материалы научно-практической конференции с международным участием, посвященной 50-летию со дня образования кафедры криминалистики юридического факультета Белорусского государственного университета. Минск, 13 апреля 2023 г. С. 341-348.

98. Янгаева М.О. Отдельные аспекты производства допросов при расследовании преступлений, связанных с использованием криптовалют // Материалы криминалистических чтений: научные основы противодействия (Долговские чтения): сб. материалов, Барнаул, 24 ноября 2022 г.: С. 89-90.

Диссертации и авторефераты диссертаций

99. Аменицкая Н.А. Взаимодействие следователя и органов, осуществляющих оперативно-розыскную деятельность в раскрытии и расследовании преступлений (в ОВД): дис. … к-та юрид. наук: 12.00.09. Нижний Новгород, 2006. 201 с.

100. Бабанина В.Г. Первоначальный этап расследования хищений в сфере дорожного строительства: дис. … к-та юрид. наук: 12.00.12. Краснодар, 2025. 227 с.

101. Бессонов А.А. Частная теория криминалистической характеристики преступлений: автореф. дис. … д-ра юрид. наук. Москва, 2017. 45 с.

102. Волчецкая Т.С. Криминалистическая ситуалогия: автореф. дис. ... д-ра юрид. наук. Москва, 1997. 48 с.

103. Драпкин, Л.Я. Построение и проверка следственных версий: автореф. дис. … к-та юрид. наук. Москва, 1972. 28 с.

104. Дьяконова О.Г. Специальные знания в судебной и иной юрисдикционной деятельности государств-членов ЕАЭС: теория и практика: дис. … д-ра юрид. наук: 12.00.12. Москва, 2021. 647 с.

105. Зеленский В.Д. Криминалистические проблемы организации расследования преступлений: дис. … д-ра юрид. наук: 12.00.09. Краснодар, 1991. 323 с.

106. Земскова А.В. Теоретические основы использования результатов оперативно-розыскной деятельности при расследовании преступлений: дис. … д-ра юрид. наук: 12.00.09. Москва, 2002. 423 с.

107. Зникин В.К. Научные основы оперативно-розыскного обеспечения раскрытия и расследования преступлений: дис. … д-ра юрид. наук: 12.00.09. Нижний Новгород, 2006. 442 с.

108. Иванова Е.В. Концептуальные основы использования специальных знаний при выявлении и расследовании преступлений, связанных с опасными для здоровья веществами: дис. ... д-ра юрид. наук: 12.00.12. Коломна, 2016. 268 с.

109. Колесниченко А.Н. Научные и правовые основы расследования отдельных видов преступлений: автореф. дис. … д-ра юрид. наук. Харьков, 1967. 27 с.

110. Нечаев В.В. Организационно-правовые основы взаимодействия органов предварительного следствия и дознания: автореферат дис. ... к-та юрид. наук: 12.00.11. Рязань, 2005. 26 с.

111. Пономарев В.Е. Технико-криминалистическое обеспечение выявления и закрепления электронных доказательств: дис. … к-та юрид. наук: 5.1.4. Краснодар, 2025. 200 с.

112. Сергеев Л.А. Расследование и предупреждение хищений, совершаемых при производстве строительных работ: автореф. дис. … к-та юрид. наук. Москва, 1966. 16 с.

113. Титов А.А. Раскрытие и расследование преступлений, совершаемых в отношении и с использованием криптовалюты (российский и зарубежный опыт): дис. … к-та юрид. наук: 5.1.4. Москва, 2025. 273 с.

Интернет-ресурсы

114. Верховный Суд РФ : сайт. URL: https://www.vsrf.ru/press_center/mass_media/34394/?ysclid=miifn7xyxr208441269 (дата обращения: 10.06.2025).

115. АО «ШАРД»: сайт. URL: https://shard.ru/services/crypto-investigations (дата обращения: 07.12.2025).

116. РБК : сайт. URL:https://www.rbc.ru/crypto/news/682f0c1f9a79474bf2e0eecd?ysclid=mg7igyfad9463994643 (дата обращения: 27.08.2025).

117. Пояснительная записка к законопроекту № 902782-8 «О внесении изменений в статью 104-1 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации (об особенностях изъятия цифровой валюты)» [Электронный ресурс] // Система обеспечения законодательной деятельности Государственной автоматизированной системы «Законотворчество» (СОЗД ГАС «Законотворчество») : сайт. URL: https://sozd.duma.gov.ru/download/1f024e33-8bca-6002-84de-5501bb89ade0 (дата обращения: 27.09.2025).

118. Пояснительная записка к законопроекту № 1065710-7 «О внесении изменений в части первую и вторую Налогового кодекса Российской Федерации и отдельные законодательные акты Российской Федерации (в части налогообложения цифровой валюты)» [Электронный ресурс] // Система обеспечения законодательной деятельности Государственной автоматизированной системы «Законотворчество» (СОЗД ГАС «Законотворчество») : сайт. URL: https://sozd.duma.gov.ru/download/2a8393c0-0964-4237-9867-36a6e01f1cd5 (дата обращения: 27.09.2025).

ПРИЛОЖЕНИЯ

Приложение 1

Анкета опроса респондентов по теме исследования

Уважаемый респондент!

В рамках диссертационного исследования по теме «Совершенствование методики первоначального этапа расследования хищений криптовалютных активов» проводится анкетирование следователей (дознавателей) и судей судов общей юрисдикции. Обращаюсь к Вам с просьбой ответить на вопросы.

Вопросы и результаты опроса по теме исследования

№	Вопрос и варианты ответов	Результат, %
1	Считаете ли Вы, что разработка и совершенствование методики расследования хищений криптовалюты является актуальной проблемой?	
	Да	95
	Нет	5

2	Знаете ли Вы, что такое криптовалюта; блокчейн; блокчейн-обозреватель; холодный криптовалютный кошелек; горячий криптовалютный кошелек; кастодиальный криптовалютный кошелек; некастодиальный криптовалютный кошелек; публичный адрес; приватный ключ; мнемоническая фраза; P2P; централизованная криптовалютная биржа; смарт-контракт; децентрализованные приложения? Если да, то сколько понятий Вам знакомо?	
	Нет	44
	Да, 1-3	44
	Да, 4-6	7
	Да, 7-9	0
	Да, 10-12	0
	Да, все перечисленные	5
3	По Вашему мнению, может ли криптовалюта быть предметом преступного посягательства?	
	Да, может	100
	Нет, не может	0
4	Как часто на практике Вы сталкиваетесь с уголовными делами о хищении криптовалюты?	
	Очень часто	0
	Часто	9
	Редко	18
	Никогда	73

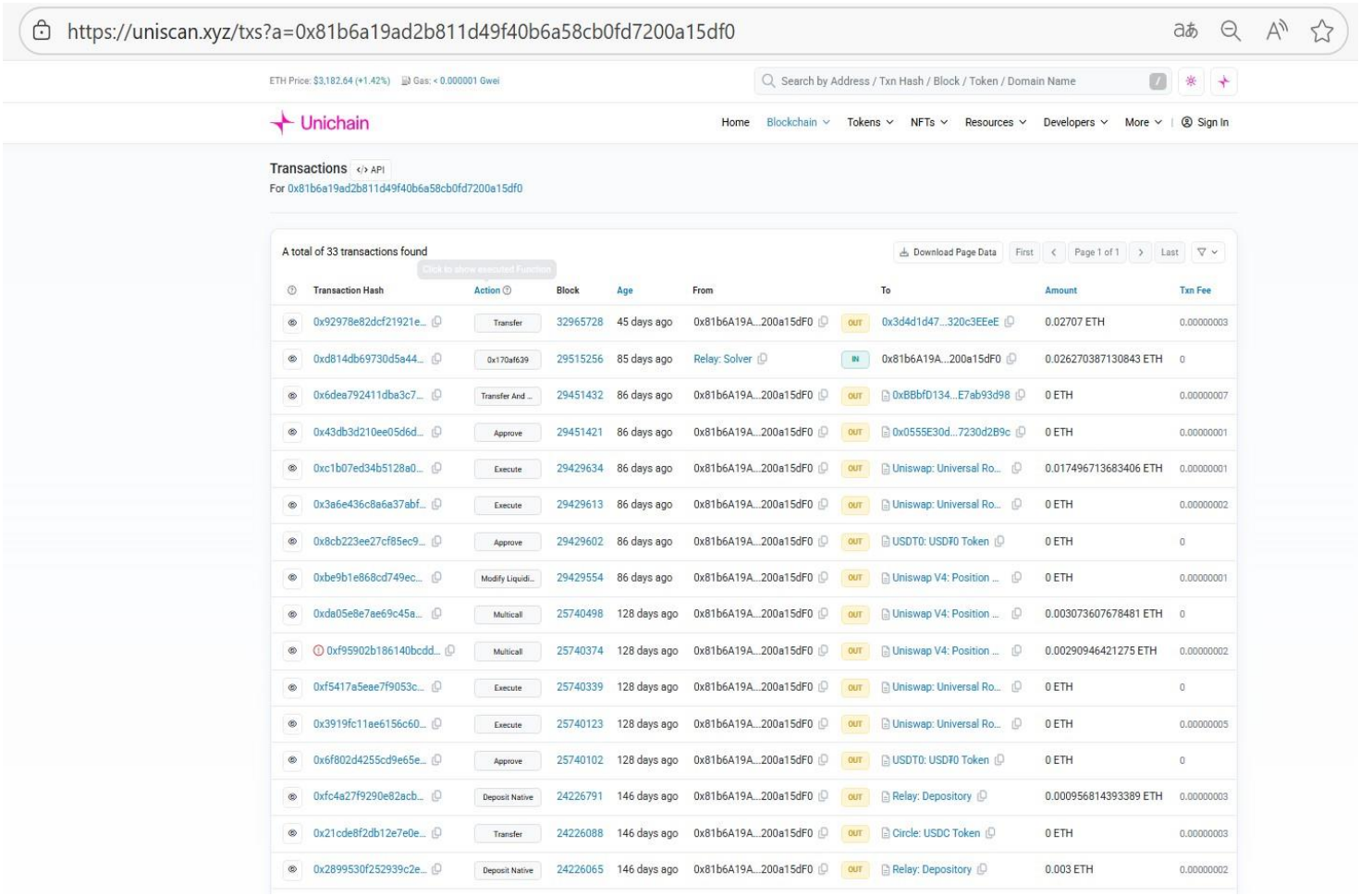
5	Нужно ли следователям и судьям обладать знаниями о понятийном аппарате криптовалютной сферы и пониманием функционирования технологии блокчейн для расследования и рассмотрения уголовных дел о хищении криптовалюты?	
	Да	95
	Нет	5
6	Какими способами происходило хищение криптовалюты по уголовным делам, находящимся в Вашем производстве?	
	Путем получения доступа к криптовалютному кошельку	8
	Путем перевода криптовалюты потерпевшим в адрес злоумышленников	17
	В результате предоставления разрешения децентрализованному приложению распоряжаться криптовалютой	2
	Не удалось установить способ хищения	0
	Таких уголовных дел в производстве не было	73
7	С выяснения каких двух обстоятельств, на Ваш взгляд, следует начинать первоначальный этап расследования хищений криптовалюты? (при условии, что потерпевший не описал каких-либо обстоятельств, имеющих значение для дела; нет никакой информации о подозреваемых лицах; установлена принадлежность похищенной криптовалюты потерпевшему, а также ее стоимость в рублевом эквиваленте)	

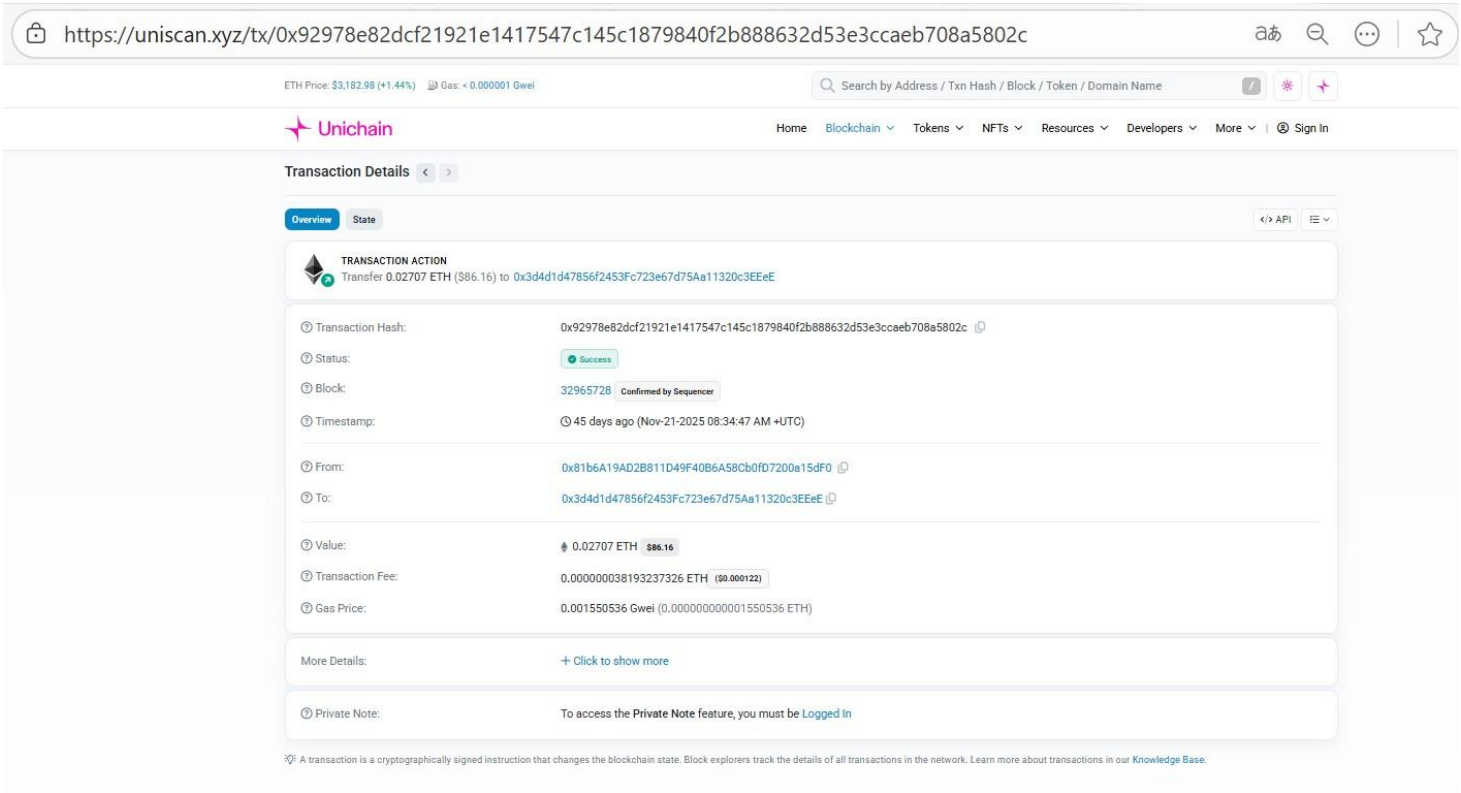
	Затрудняюсь ответить	50
	Наличие или отсутствие вредоносного программного обеспечения на устройстве потерпевшего; Наличие или отсутствие переписок с потенциальными злоумышленниками	17
	Способ хранения криптовалюты; Осуществлен ли перевод в адрес злоумышленника самостоятельно или нет	25
	Осуществлялась ли передача данных для доступа к кошельку посторонним; Кому принадлежит кошелек, в адрес которого поступила похищенная криптовалюта	8
8	Сталкивались ли Вы с уголовными делами о хищении криптовалюты, в которых не было ничего известно о личности подозреваемого? Если да, то удалось ли установить их личность?	
	Нет	80
	Да, удалось	0
	Да, не удалось	20
9	Сталкивались ли Вы с материалами проверки сообщений о хищении криптовалюты? Если да, то принимались ли решения об отказе в возбуждении уголовного дела? В связи с чем?	
	Нет	83
	Да, принимались в связи с отсутствием достаточных оснований (отсутствие события или состава и т.д.)	17
		0

	Да, принимались в связи с тем, что криптовалюта не имеет правового статуса на территории РФ и не может быть признана имуществом	
10	Какие действия Вы производили на этапе проверки сообщений о хищении криптовалюты?	
	Получение объяснения от заявителя	23
	Получение объяснения от других лиц	12
	Осмотр места происшествия	1
	Осмотр электронных устройств	13
	Назначение экспертизы	0
	Направление запроса в адрес организаций	16
	Поручение о проведении ОРМ	23
	Таких материалов проверок в производстве не было	12
11	Является ли, на Ваш взгляд, обязательным осмотр блокчейн-обозревателей (в рамках осмотра электронных устройств) в ходе расследования (рассмотрения) уголовных дел о хищении криптовалюты?	
	Да, является	49
	Нет, не является	2
	Затрудняюсь ответить	49
12	Является ли, на Ваш взгляд, обязательным осмотр криптовалютных кошельков (в рамках осмотра электронных устройств) в ходе расследования (рассмотрения) уголовных дел о хищении криптовалюты?	
	Да, является	54

	Нет, не является	5
	Затрудняюсь ответить	41
13	Является ли, на Ваш взгляд, обязательным назначение экспертиз (экономической, компьютерно-технической) в ходе расследования (рассмотрения) уголовных дел о хищении криптовалюты?	
	Да, является, в большинстве случаев	67
	Нет, не является	10
	Затрудняюсь ответить	23
14	Направляли ли Вы запросы в адрес криптовалютных бирж, зарегистрированных на территории иностранных государств, о предоставлении информации о лице, использовавшем биржевой (кастодиальный) кошелек? Если да, то были ли получены ответы?	
	Да, ответы получены	3
	Да, ответы не получены	7
	Нет, не было необходимости	17
	Нет, так как в производстве не было таких уголовных дел	73
15	Сталкивались ли Вы с ситуацией, когда производство всех возможных действий по уголовным делам о хищении криптовалюты не дало результата по установлению личностей подозреваемых?	
	Да	33
	Нет	67

16	На Ваш взгляд, достаточно ли в настоящее время в органах предварительного расследования квалифицированных кадров, способных эффективно расследовать хищения криптовалюты (особенно, в условиях, когда нет никакой информации о личности подозреваемого или этой информации крайне мало) *Достаточно* *Недостаточно* *Их нет*	 0 83 17
17	На Ваш взгляд, есть ли в настоящее время необходимость в пополнении подразделений органов предварительного расследования кадрами, обладающими познаниями о специфике взаимодействия с криптовалютой / повышении квалификации действующих сотрудников в части взаимодействия с криптовалютой? *Да, есть* *Нет*	 92 8
18	На Ваш взгляд, есть ли в настоящее время необходимость в создании специализированных подразделений органов предварительного расследования, специализирующихся на расследовании преступлений, которые совершены с использованием криптовалюты? *Да, есть* *Нет*	 75 25


https://uniscan.xyz/txs?a=0x81b6a19ad2b811d49f40b6a58cb0fd7200a15df0
ETH Price: $3,182.64 (+1.42%) Gas: < 0.000001 Gwei
Search by Address / Txn Hash / Block / Token / Domain Name
Unichain
Home Blockchain Tokens NFTs Resources Developers More Sign In
Transactions API
For 0x81b6a19ad2b811d49f40b6a58cb0fd7200a15df0
A total of 33 transactions found
Download Page Data First Page 1 of 1 Last
Transaction Hash Action Block Age From To Amount Txn Fee
0x92978e82dcf21921e... Transfer 32965728 45 days ago 0x81b6A19A...200a15dF0 OUT 0x3d4d1d47...320c3EEeE 0.02707 ETH 0.00000003
0xd814db69730d5a44... 0x170af639 29515256 85 days ago Relay: Solver IN 0x81b6A19A...200a15dF0 0.026270387130843 ETH 0
0x6dea792411dba3c7... Transfer And ... 29451432 86 days ago 0x81b6A19A...200a15dF0 OUT 0xBBbfD134...E7ab93d98 0 ETH 0.00000007
0x43db3d210ee05d6d... Approve 29451421 86 days ago 0x81b6A19A...200a15dF0 OUT 0x0555E30d...7230d2B9c 0 ETH 0.00000001
0xc1b07ed34b5128a0... Execute 29429634 86 days ago 0x81b6A19A...200a15dF0 OUT Uniswap: Universal Ro... 0.017496713683406 ETH 0.00000001
0x3a6e436c8a6a37abf... Execute 29429613 86 days ago 0x81b6A19A...200a15dF0 OUT Uniswap: Universal Ro... 0 ETH 0.00000002
0x8cb223ee27cf85ec9... Approve 29429602 86 days ago 0x81b6A19A...200a15dF0 OUT USDT0: USD₮0 Token 0 ETH 0
0xbe9b1e868cd749ec... Modify Liquidi... 29429554 86 days ago 0x81b6A19A...200a15dF0 OUT Uniswap V4: Position ... 0 ETH 0.00000001
0xda05e8e7ae69c45a... Multicall 25740498 128 days ago 0x81b6A19A...200a15dF0 OUT Uniswap V4: Position ... 0.003073607678481 ETH 0
0xf95902b186140bcdd... Multicall 25740374 128 days ago 0x81b6A19A...200a15dF0 OUT Uniswap V4: Position ... 0.00290946421275 ETH 0.00000002
0xf5417a5eae7f9053c... Execute 25740339 128 days ago 0x81b6A19A...200a15dF0 OUT Uniswap: Universal Ro... 0 ETH 0
0x3919fc11ae6156c60... Execute 25740123 128 days ago 0x81b6A19A...200a15dF0 OUT Uniswap: Universal Ro... 0 ETH 0.00000005
0x6f802d4255cd9e65e... Approve 25740102 128 days ago 0x81b6A19A...200a15dF0 OUT USDT0: USD₮0 Token 0 ETH 0
0xfc4a27f9290e82acb... Deposit Native 24226791 146 days ago 0x81b6A19A...200a15dF0 OUT Relay: Depository 0.000956814393389 ETH 0.00000003
0x21cde8f2db12e7e0e... Transfer 24226088 146 days ago 0x81b6A19A...200a15dF0 OUT Circle: USDC Token 0 ETH 0.00000003
0x2899530f252939c2e... Deposit Native 24226065 146 days ago 0x81b6A19A...200a15dF0 OUT Relay: Depository 0.003 ETH 0.00000002


https://uniscan.xyz/tx/0x92978e82dcf21921e1417547c145c1879840f2b888632d53e3ccaeb708a5802c
ETH Price: $3,182.98 (+1.44%)
Gas: < 0.000001 Gwei
Search by Address / Txn Hash / Block / Token / Domain Name
Unichain
Home
Blockchain
Tokens
NFTs
Resources
Developers
More
Sign In
Transaction Details
Overview
State
API
TRANSACTION ACTION
Transfer 0.02707 ETH ($86.16) to 0x3d4d1d47856f2453Fc723e67d75Aa11320c3EEeE
Transaction Hash:
0x92978e82dcf21921e1417547c145c1879840f2b888632d53e3ccaeb708a5802c
Status:
Success
Block:
32965728
Confirmed by Sequencer
Timestamp:
45 days ago (Nov-21-2025 08:34:47 AM +UTC)
From:
0x81b6A19AD2B811D49F40B6A58Cb0fD7200a15dF0
To:
0x3d4d1d47856f2453Fc723e67d75Aa11320c3EEeE
Value:
0.02707 ETH
$86.16
Transaction Fee:
0.000000038193237326 ETH
($0.000122)
Gas Price:
0.001550536 Gwei (0.000000000001550536 ETH)
More Details:
+ Click to show more
Private Note:
To access the Private Note feature, you must be Logged In
A transaction is a cryptographically signed instruction that changes the blockchain state. Block explorers track the details of all transactions in the network. Learn more about transactions in our Knowledge Base.

Приложение 4