

Федеральное государственное казенное образовательное учреждение
высшего образования «Сибирский юридический институт
Министерства внутренних дел Российской Федерации»

Кафедра криминалистики

Специальность 40.05.02 Правоохранительная деятельность
(специализация «Оперативно-розыскная деятельность», профиль
образовательной программы — «Деятельность
оперуполномоченного уголовного розыска»)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

по теме:

**МЕТОДИКА РАССЛЕДОВАНИЯ ЛЕГАЛИЗАЦИИ ДЕНЕЖНЫХ СРЕДСТВ
И ИНОГО ИМУЩЕСТВА, СОВЕРШЕННОЙ С ИСПОЛЬЗОВАНИЕМ
КРИПТОВАЛЮТЫ И ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СРЕДСТВ**

Выполнил:

Слушатель группы П 2102-УР
младший лейтенант полиции
Красильников Илья Алексеевич

Руководитель:

Доцент кафедры криминалистики,
кандидат юридических наук
Гарбуз Григорий Сергеевич

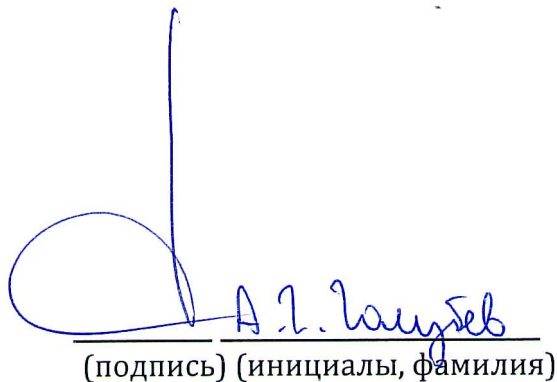
Дата защиты:

«14» июня 2026 г.

Оценка: отлично

Председатель ГЭК

Иванович Иван Иванович
(специальное звание)


(подпись) (инициалы, фамилия)

Красноярск 2026

Федеральное государственное казенное образовательное учреждение
высшего образования «Сибирский юридический институт
Министерства внутренних дел Российской Федерации»

Кафедра криминалистики

Специальность 40.05.02 Правоохранительная деятельность
(специализация «Оперативно-розыскная деятельность», профиль
образовательной программы — «Деятельность
оперуполномоченного уголовного розыска»)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
по теме:
МЕТОДИКА РАССЛЕДОВАНИЯ ЛЕГАЛИЗАЦИИ ДЕНЕЖНЫХ
СРЕДСТВ
И ИНОГО ИМУЩЕСТВА, СОВЕРШЕННОЙ С ИСПОЛЬЗОВАНИЕМ
КРИПТОВАЛЮТЫ И ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СРЕДСТВ

Выполнил:

Слушатель группы П 2102-УР
младший лейтенант полиции
Красильников Илья Алексеевич

Руководитель:

Доцент кафедры криминалистики,
кандидат юридических наук
Гарбуз Григорий Сергеевич

Дата защиты:

«___» _____ 2026 г.

Оценка: _____

Председатель ГЭК

(специальное звание)

(подпись) (инициалы, фамилия)

Красноярск 2026

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ.....	3
ГЛАВА 1. ТЕОРЕТИКО-ПРАВОВЫЕ ОСНОВЫ РАССЛЕДОВАНИЯ ЛЕГАЛИЗАЦИИ ДЕНЕЖНЫХ СРЕДСТВ И ИНОГО ИМУЩЕСТВА, СОВЕРШЕННОЙ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТЫ И ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СРЕДСТВ	9
§1. Уголовно-правовая характеристика легализации денежных средств и иного имущества	9
§2. Правовой режим криптовалюты и электронных платежных средств ...	15
§3. Криминалистическая классификация легализации денежных средств и иного имущества, совершенной с использованием криптовалюты и электронных платежных средств.....	22
ГЛАВА 2. МЕТОДИКА РАССЛЕДОВАНИЯ ЛЕГАЛИЗАЦИИ ДЕНЕЖНЫХ СРЕДСТВ И ИНОГО ИМУЩЕСТВА, СОВЕРШЕННОЙ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТЫ И ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СРЕДСТВ.....	28
§1. Криминалистическая характеристика легализации денежных средств и иного имущества, совершенной с использованием криптовалюты и электронных платежных средств.....	28
§2. Типичные следственные ситуации легализации денежных средств и иного имущества, совершенной с использованием криптовалюты и электронных платежных средств.....	37
§3. Система тактических задач и способы их решения легализации денежных средств и иного имущества, совершенной с использованием криптовалюты и электронных платежных средств	43
§4. Криминалистические особенности легализации денежных средств и иного имущества, совершенной с использованием криптовалюты и электронных платежных средств.....	50
ЗАКЛЮЧЕНИЕ	56
СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ.....	62

ВВЕДЕНИЕ

Актуальность темы исследования. В условиях стремительного развития цифровых технологий и внедрения новых финансовых инструментов легализация (отмывание) денежных средств и иного имущества, совершаемая с использованием криптовалюты и электронных платежных средств, приобретает повышенную общественную опасность и становится одной из ключевых угроз устойчивости национальной финансовой системы как Российской Федерации, так и мирового сообщества в целом. Использование распределенных реестров, анонимных электронных кошельков, сервисов микширования и трансграничных цифровых платежей существенно осложняет выявление преступных доходов, их прослеживаемость и документирование противоправной деятельности.

В соответствии с актуальными статистическими данными МВД России за 2025 год¹ и январь–май 2026 года² количество зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, снизилось. Вместе с тем указанная динамика не устраняет актуальность темы исследования, поскольку легализация преступных доходов с использованием цифровых финансовых инструментов сохраняет высокую латентность, трансграничный характер и доказательственную сложность. Использование электронных кошельков, P2P-обменников, криптовалютных сервисов и распределенных реестров затрудняет установление происхождения

¹ Статистические сведения о состоянии преступности в 2025 году // МВД МЕДИА : [Электронный ресурс]. – 29.01.2026. – URL: <https://mvdmedia.ru/news/official/statisticheskie-svedeniya-o-sostoyanii-prestupnosti-v-2025-godu/> (дата обращения: 18.06.2026).

² МВД России публикует статистическую информацию о состоянии преступности в Российской Федерации за январь–май 2026 года // МВД МЕДИА : [Электронный ресурс]. – 17.06.2026. – URL: <https://mvdmedia.ru/news/official/mvd-rossii-publikuet-statisticheskuyu-informatsiyu-o-sostoyanii-prestupnosti-/> (дата обращения: 18.06.2026).

имущества, маршрута движения активов и круга причастных лиц. Поэтому актуальность темы определяется не только количественными показателями преступности, но и качественной трансформацией способов легализации преступных доходов в цифровой среде.

Научная новизна исследования заключается в комплексном криминалистическом анализе методики расследования легализации денежных средств и иного имущества, совершаемой с использованием криптовалюты и электронных платежных средств, с учетом современных цифровых способов совершения преступлений, особенностей формирования цифровых следов и возможностей их использования в процессе доказывания, а также в разработке практико-ориентированных рекомендаций для следственных подразделений органов внутренних дел.

Теоретическая значимость работы состоит в развитии положений частной криминалистической методики расследования преступлений в сфере экономической деятельности и формировании научных подходов к расследованию легализации преступных доходов, совершаемой с применением цифровых финансовых инструментов.

Практическая значимость исследования заключается в возможности использования сформулированных выводов и рекомендаций:

- в деятельности следственных подразделений органов внутренних дел;
- при разработке ведомственных методических рекомендаций;
- в учебном процессе образовательных организаций системы МВД России.

Указ Президента РФ от 2 июля 2021 г. № 400 «О стратегии национальной безопасности Российской Федерации» закрепляет предупреждение и пресечение преступлений в сфере легализации преступных доходов как одну из основных задач государства. А также утверждается, что информационно-телекоммуникационные технологии обеспечивают анонимность и облегчают совершение преступлений, связанных с легализацией денежных средств.

Указ Президента РФ от 13 мая 2017 г. № 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года» также закрепляет противодействие легализации доходов, полученных преступным путем как одну из основных задач по реализации устойчивого развития национальной финансовой системы государства.

Концепция развития национальной системы противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, утвержденная Президентом РФ 30 мая 2018 г. закрепляет основные задачи по снижению уровня преступности, связанной с легализацией (отмыванием) доходов, полученных преступным путем: развитие методик предупреждения, выявления, расследования и раскрытия преступлений; введение для следователей, судов и прокуроров специализации для расследования уголовных дел в данной сфере и повышение их квалификации в этой области; совершенствование судебно-экспертных учреждений в сфере расследования и рассмотрения уголовных дел, связанных с легализацией доходов, полученных преступным путем.

Цель и задачи исследования. Целью данной работы является изучение и комплексный анализ теоретической базы криминалистической методики расследования легализации денежных средств и иного имущества, совершенной с использованием криптовалюты и электронных платежных средств, а также анализ следственной и судебной практики с целью разработки рекомендаций для повышения эффективности расследования данных уголовных дел в практической деятельности правоохранительных органов.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Изучение теоретических основ криминалистической методики расследования легализации денежных средств и иного имущества, совершенной с использованием криптовалюты и электронных платежных средств.

2. Анализ нормативно-правовой базы и методических рекомендаций, регулирующих методику расследования легализации денежных средств и иного имущества, совершенной с использованием криптовалюты и электронных платежных средств.

3. Выявление особенностей криминалистической методики расследования легализации денежных средств и иного имущества, совершенной с использованием криптовалюты и электронных платежных средств, а также анализ и использование цифровых доказательств.

4. Изучение основных проблем и типичных ошибок, которые возникают в следственной и судебной практике при расследовании легализации денежных средств и иного имущества, совершенной с использованием криптовалюты и электронных платежных средств, а также определение причин их возникновения.

5. Разработка рекомендаций по совершенствованию методики расследования легализации денежных средств и иного имущества, совершенной с использованием криптовалюты и электронных платежных средств.

6. Анализ зарубежного опыта противодействия легализации преступных доходов с применением криптовалют.

7. Разработка рекомендаций по использованию современных технических средств и экспертных методов при расследовании.

Объектом исследования выступают общественные отношения, возникающие в связи с противодействием легализации (отмыванием) денежных средств и иного имущества, совершенной с использованием криптовалюты и электронных платежных средств.

Предметом исследования являются закономерности выявления, раскрытия и расследования легализации денежных средств и иного имущества, совершенной с использованием криптовалюты и электронных платежных средств, а также особенности использования цифровых следов и специальных знаний при доказывании указанных деяний.

Методологической основой исследования являются общенаучные методы (анализ, синтез, сравнение, обобщение, индукция, дедукция), частно-научные методы (сравнительный анализ, формально-юридический и сравнительно-правовой методы), а также специальные методы криминалистики (формально-логические, статистические, экспертные). В работе использованы материалы уголовных дел, судебной практики, научные труды отечественных и зарубежных криминалистов, а также нормативные правовые акты.

Степень разработанности данной темы является достаточно обширной. Теоретическую базу исследования составляют труды таких ученых, как Р.С. Белкин, Н.В. Вильская, В.П. Гурская, С.И. Земцова, В.Е. Корноухов, А.В. Макаров, А.И. Миллюс, В.Ю. Малахов, Д.Е. Некрасов, Л.Д. Родионов, А.Г. Филиппов, А.В. Шашков и многих других.

Нормативную базу исследования составляют: Конституция Российской Федерации, Уголовный кодекс Российской Федерации, Уголовно-процессуальный кодекс Российской Федерации, Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе», Федеральный закон от 31.07.2020 № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации», а также федеральные законы 2024–2026 гг., конкретизирующие правовой режим цифровой валюты, майнинга, экспериментальных расчетов цифровой валютой и порядок ареста и изъятия цифровой валюты в уголовном судопроизводстве.

Эмпирическую базу исследования составили материалы судебной и следственной практики по уголовным делам о легализации преступных

доходов, в том числе с использованием информационно-телекоммуникационных технологий.

Структура работы обусловлена целью и задачами исследования.

Во введении обосновывается актуальность темы, определяются цель, задачи, объект и предмет исследования, раскрываются методологическая, нормативная и эмпирическая основы работы.

В первой главе рассматриваются теоретико-правовые основы расследования легализации преступных доходов, раскрываются уголовно-правовая характеристика данных преступлений, правовое регулирование оборота криптовалюты и электронных платежных средств, а также криминалистическая классификация указанных деяний.

Во второй главе исследуются элементы частной криминалистической методики расследования легализации преступных доходов, дается криминалистическая характеристика, анализируются типичные следственные ситуации, формируется система тактических задач первоначального этапа расследования и рассматриваются особенности производства отдельных следственных действий.

В заключении подводятся итоги проведенного исследования, формулируются основные выводы и практические рекомендации.

ГЛАВА 1. ТЕОРЕТИКО-ПРАВОВЫЕ ОСНОВЫ РАССЛЕДОВАНИЯ ЛЕГАЛИЗАЦИИ ДЕНЕЖНЫХ СРЕДСТВ И ИНОГО ИМУЩЕСТВА, СОВЕРШЕННОЙ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТЫ И ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СРЕДСТВ

1.1. Уголовно-правовая характеристика легализации денежных средств и иного имущества

Термин легализация (отмывание) официально возник в 1920-е годы в США в связи с выявлением деятельности Альфонса Капоне, а именно смешивание преступных денежных средств и выручки сети прачечных самообслуживания¹.

Если рассматривать российскую историю, то в Псковской судной грамоте 1467 года термин «легализация» отсутствует, однако его сущность прослеживается через разграничение законных и незаконных способов приобретения имущества. Законность сделки подтверждалась показаниями свидетелей либо присягой. Судебник 1550 года расширил перечень способов подтверждения законности сделки: дополнительным средством выступало поручительство за продавца. Если предыдущие правовые акты преимущественно обеспечивали законность гражданского оборота, то Соборное уложение 1649 года уже юридически закрепило ответственность за прием, хранение или продажу похищенного имущества, то есть фактически устанавливало запрет на легализацию имущества, полученного преступным путем. Данный запрет также прослеживается в Уложении о наказаниях

¹ Шашкова, А.В. Зарождение понятия «легализация (отмывание) доходов, полученных преступным путем» / А.В. Шашкова // Вестник МГИМО. – 2011. – № 3. – С. 272–274.

уголовных и исправительных 1885 года, положения которого близки к современному пониманию легализации преступных доходов.

В настоящее время легализация денежных средств и иного имущества, полученных преступным путем, представляет собой сложное социально-правовое явление, непосредственно связанное с функционированием теневого сектора экономики и обеспечением воспроизводства преступной деятельности. В современных условиях данное преступление приобретает повышенную общественную опасность, поскольку позволяет не только сохранить незаконно полученные активы, но и интегрировать их в легальный финансово-экономический оборот, создавая тем самым материальную основу для дальнейшего совершения преступлений.

В соответствии с Федеральным законом от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» под легализацией (отмыванием) доходов, полученных преступным путем понимается придание правомерного вида владению, пользованию или распоряжению денежными средствами или иным имуществом, полученными в результате совершения преступления.

Уголовная ответственность за указанные деяния установлена статьями 174 и 174.1 Уголовного кодекса Российской Федерации. Их разграничение осуществляется по субъекту преступления: в первом случае ответственность наступает за совершение финансовых операций с имуществом, заведомо приобретенным преступным путем другими лицами, во втором — за действия по легализации доходов лицом, непосредственно совершившим предикатное преступление. Такая конструкция уголовно-правовых норм соответствует международным стандартам, выработанным ФАТФ, и направлена на обеспечение комплексного противодействия вовлечению криминальных доходов в легальный оборот.

Непосредственным объектом рассматриваемых преступлений выступают общественные отношения, обеспечивающие установленный

порядок осуществления экономической деятельности и стабильность финансовой системы. Одновременно легализация посягает на интересы правосудия, поскольку сокрытие преступного происхождения имущества существенно затрудняет выявление и расследование предикатных преступлений.

Предметом преступления являются денежные средства и иное имущество, полученные в результате совершения преступления. В правоприменительной практике установление их криминального происхождения представляет значительную сложность. Как разъяснено в Постановлении Пленума Верховного Суда РФ от 07.07.2015 № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем», для квалификации по статьям 174 и 174.1 УК РФ не требуется наличие вступившего в законную силу обвинительного приговора, однако суд должен установить факт преступного происхождения имущества. Данное положение имеет принципиальное значение для деятельности следователя, поскольку определяет специфику предмета доказывания по уголовным делам данной категории.

В соответствии с вышеуказанным Постановлением Пленума Верховного Суда от 07.07.2015 № 32 к денежным средствам относят наличные денежные средства в валюте Российской Федерации или в иностранной валюте, а также безналичные денежные средства, в том числе электронные денежные средства. Если наличные денежные средства – это монеты или бумажные банкноты, которые находятся в свободном обращении и представляют собой материальный предмет, который можно потрогать, то с безналичными денежными средствами и электронными денежными средствами дела обстоят сложнее, так как они являются бестелесными вещами (*res incorporales*).

Основные отличия безналичных денежных средств и электронных денежных средств:

- безналичные денежные средства хранятся на банковском счете, тогда как электронные денежные средства в электронном кошельке;

- безналичные денежные средства рассматриваются как права требования к банковским организациям, в отличие от электронных денежных средств, которые представляют собой права требования владельца к оператору электронных денежных средств об их погашении¹;

- перед осуществлением операций с электронными денежными средствами производится их предварительная оплата традиционными формами денег, в то время как для проведения операций с безналичными денежными средствами необходимо их предварительное внесение в банк².

Таким образом, под электронными денежными средствами понимается платежный механизм, в цифровой форме хранящий денежную стоимость на сервере или специализированном устройстве, для их использования требуется применение электронных средств платежа. Законодательное определение электронных денежных средств закреплено в пункте 18 части 1 статьи 3 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе». Некоторые ученые также придерживаются мнения, что электронные денежные средства являются разновидностью безналичных³.

Под иным имуществом в соответствии с Постановлением Пленума Верховного Суда РФ от 07.07.2015 № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем» понимается движимое и недвижимое имущество, имущественные права, документарные и бездокументарные

¹ Некрасов, Д.Е. Электронные денежные средства как предмет преступления / Д.Е. Некрасов, А.А. Брюханов, И.П. Напханенко // ЮП. – 2023. – № 4 (107). – С. 167–174.

² Архипов, А.В. Ответственность за хищение безналичных и электронных денежных средств: новеллы законодательства / А.В. Архипов // Уголовное право. – 2018. – № 3. – С. 4–9.

³ Макаров, А.В. Особенности и проблемы квалификации мошенничества, совершенного с использованием электронных средств платежа / А.В. Макаров, В.А. Алешкова // Российский судья. – 2019. – № 5. – С. 24–29.

ценные бумаги, а также имущество, полученное в результате переработки имущества, приобретённого преступным путем или в результате совершения преступления.

Имущество должно обладать тремя значимыми признаками: физическим (предмет внешнего мира, доступный для восприятия), юридическим (предмет правового обладания физического или юридического лица, составляющий его собственность) и экономическим (предмет гражданского оборота).

Вместе с тем наличие специальных ограничений оборота цифровой валюты само по себе не исключает ее признание имуществом для целей уголовного и уголовно-процессуального законодательства. После внесения изменений Федеральным законом от 20.02.2026 № 38-ФЗ цифровая валюта прямо признается имуществом для целей УК РФ и УПК РФ, что имеет значение для квалификации легализации, конфискации, наложения ареста и изъятия цифровой валюты.

Дополнительное значение для определения предмета преступлений, совершаемых в цифровой среде, имеют разъяснения Постановления Пленума Верховного Суда Российской Федерации от 16 июня 2026 г. № 30 «О внесении изменений в некоторые постановления Пленума Верховного Суда Российской Федерации по уголовным делам». Верховный Суд Российской Федерации уточнил, что предметом хищения наряду с наличными и безналичными денежными средствами могут выступать цифровые права и цифровая валюта, если они обладают экономической ценностью и находятся под контролем потерпевшего. Для расследования легализации данная позиция важна при установлении цифровой валюты в качестве имущества, полученного в результате предикатного преступления, и последующем доказывании ее преступного происхождения¹.

¹ О внесении изменений в некоторые постановления Пленума Верховного Суда Российской Федерации по уголовным делам : постановление Пленума Верховного Суда Российской Федерации от 16.06.2026 № 30 // СПС КонсультантПлюс.

Объективная сторона легализации выражается в совершении финансовых операций и иных сделок с преступно приобретенным имуществом, а также в использовании его в предпринимательской или иной экономической деятельности. Юридически значимыми признаются любые действия, направленные на создание видимости законности происхождения соответствующих активов. На практике такие действия реализуются посредством сложных финансовых схем, включающих многоступенчатые переводы денежных средств, их дробление, использование подконтрольных организаций, заключение фиктивных гражданско-правовых договоров, а также привлечение номинальных лиц.

Состав преступления является формальным и считается оконченным с момента совершения соответствующей финансовой операции либо иной сделки независимо от фактического достижения цели легализации. Указанное обстоятельство позволяет пресекать преступную деятельность на ранних стадиях.

С субъективной стороны легализация характеризуется прямым умыслом и наличием специальной цели — придания правомерного вида владению, пользованию и распоряжению преступно приобретенным имуществом. Именно наличие данной цели позволяет отграничить легализацию от иных преступлений, связанных с распоряжением похищенным имуществом. Использование денежных средств для личного потребления без придания им признаков законности, как правило, не образует состава легализации.

Субъект преступления является общим. Квалифицирующими признаками выступают совершение деяния группой лиц по предварительному сговору либо организованной группой, использование служебного положения, а также крупный и особо крупный размер. Наличие указанных обстоятельств свидетельствует о системном характере легализации и ее тесной связи с организованной преступной деятельностью.

Н.А. Лопашенко обоснованно подчеркивает производный характер легализации. Вместе с тем последующие действия по приданию правомерного

вида преступным доходам образуют самостоятельный состав преступления и подлежат квалификации по совокупности, поскольку посягают на иной объект уголовно-правовой охраны¹.

Современный этап развития финансовых технологий обусловил появление новых форм предмета легализации. Цифровые активы, несмотря на специфику их правового режима, обладают имущественной ценностью и могут использоваться в целях сокрытия преступного происхождения денежных средств, их конвертации и перемещения между различными юрисдикциями. Указанное обстоятельство предопределяет необходимость учета особенностей их использования при квалификации соответствующих деяний и разработке методики расследования.

Таким образом, уголовно-правовая характеристика легализации денежных средств и иного имущества определяется совокупностью признаков, отражающих производный характер данного преступления, его направленность на придание правомерного вида преступным доходам и вовлечение их в легальный экономический оборот. Установление указанных обстоятельств формирует основу предмета доказывания и предопределяет выбор тактики расследования по уголовным делам данной категории.

1.2. Правовой режим криптовалюты и электронных платежных средств

История криптовалюты берет свое начало с 1980–1990-х годов, когда зарождались теоретические представления о цифровых деньгах. Дэвид Чаум в 1989 году разработал систему, обеспечивавшую анонимность цифровых транзакций – DigiCash. В 2008 году анонимный разработчик под псевдонимом

¹ Лопашенко Н.А. Преступления в сфере экономической деятельности: теоретический и прикладной анализ : монография. – Ч. 1. – М. : Юрлитинформ, 2015. – 330 с.

Сатоши Накамото представил миру работу, в которой описывалась децентрализованная система электронных денег, функционирующая на базе технологии блокчейн (криптографическая система, которая содержит информацию обо всех транзакциях, проведенных ее участниками), а на следующий год этот же разработчик представляет всему миру первую криптовалюту – Bitcoin (Биткойн). С 2009 по настоящее время идет бурный рост рынка криптовалют¹.

На данный момент криптовалюта вышла на новый уровень и стала значительно влиять на финансовые отношения как в России, так и во всем мире, а также вызывает множество споров и дискуссий в научных кругах. В законодательстве Российской Федерации термин «криптовалюта» прямо не используется как базовая юридическая категория, однако Федеральный закон от 31.07.2020 № 259-ФЗ закрепляет правовой режим цифровой валюты². Согласно указанному закону под цифровой валютой понимается совокупность электронных данных (цифрового кода или обозначения), содержащихся в информационной системе, которые могут использоваться в качестве средства платежа, не являющегося денежной единицей, и (или) в качестве инвестиций; при этом отсутствует лицо, обязанное перед каждым обладателем таких электронных данных. Согласно части 11 статьи 1 Федерального закона «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» к цифровой валюте не относятся безналичные денежные средства, электронные денежные средства и бездокументарные ценные бумаги.

¹ Земцова, С.И. Криптовалюта как объект криминалистического исследования при расследовании преступлений в сфере незаконного оборота наркотических средств и психотропных веществ : учебное пособие / С.И. Земцова, П.В. Галушин, А.Л. Карлов. – Красноярск : СибЮИ МВД России, 2021. – 104 с.

² О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 31.07.2020 № 259-ФЗ // СПС КонсультантПлюс.

Правовой режим цифровой валюты был существенно конкретизирован изменениями 2024–2026 гг. Федеральным законом от 08.08.2024 № 221-ФЗ введены правовые основы майнинга цифровой валюты, майнинг-пула и деятельности операторов майнинговой инфраструктуры. Юридические лица и индивидуальные предприниматели вправе осуществлять майнинг после включения в соответствующий реестр, а физические лица — граждане Российской Федерации могут осуществлять майнинг без включения в реестр при соблюдении лимитов энергопотребления, установленных Правительством Российской Федерации.

Федеральным законом от 25.10.2024 № 349-ФЗ уточнен порядок государственного контроля за майнингом: ФНС России ведет реестры майнеров и операторов майнинговой инфраструктуры, а лица, осуществляющие майнинг, обязаны представлять сведения о получении цифровой валюты и об адресах-идентификаторах. Указанные сведения могут иметь значение для выявления операций, связанных с легализацией преступных доходов, поскольку позволяют устанавливать связь между субъектом, цифровой валютой и конкретными адресами в блокчейн-сети.

Дополнительное значение имеет Постановление Правительства Российской Федерации от 18.03.2026 № 280, которым продлен срок действия запрета на осуществление майнинга цифровой валюты, в том числе участие в майнинг-пуле, на отдельных территориях Республики Бурятия и Забайкальского края с 1 апреля 2026 года по 15 марта 2031 года. Для темы исследования это важно не само по себе как ограничение энергопотребления, а как подтверждение формирования более детального режима государственного контроля за инфраструктурой получения и оборота цифровой валюты.¹

¹ О внесении изменения в постановление Правительства Российской Федерации от 23 декабря 2024 г. № 1869 : постановление Правительства Российской Федерации от 18.03.2026 № 280. Доступ из справочной правовой системы «КонсультантПлюс».

Отдельное значение имеет Федеральный закон от 08.08.2024 № 223-ФЗ, которым Банк России наделен полномочиями по установлению экспериментальных правовых режимов для операций с цифровой валютой, в том числе при внешнеторговых расчетах и организованных торгах цифровой валютой. Следовательно, в работе необходимо разграничивать общий запрет на использование цифровой валюты как встречного предоставления за товары, работы и услуги внутри Российской Федерации и специальные случаи использования цифровой валюты в рамках экспериментального правового режима.

Федеральным законом от 20.02.2026 № 38-ФЗ цифровая валюта признана имуществом для целей уголовного и уголовно-процессуального законодательства. Это означает, что при расследовании легализации преступных доходов цифровая валюта может рассматриваться не только как технологический способ перемещения стоимости, но и как возможный предмет преступления, объект ареста, изъятия и конфискации.

С учетом Постановления Пленума Верховного Суда РФ от 07.07.2015 № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем», статьи 1 Конвенции Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности и о финансировании терроризма от 16 мая 2005 года, а также Рекомендации 15 ФАТФ денежные средства, преобразованные из виртуальных активов (криптовалюты), полученных в результате преступной деятельности, могут являться предметом преступления.

Таким образом, под криптовалютой в криминалистическом аспекте можно понимать разновидность цифровой децентрализованной валюты, функционирующей в автоматизированном режиме, не имеющей физического выражения и основанной на механизме блокчейна. Она существует в виде цифрового значения, отражающего объем расчетных единиц и фиксируемого

в информационной системе. Сведения о транзакциях, как правило, передаются и сохраняются в открытом виде, однако идентификация конкретных участников оборота осложняется псевдонимным характером адресов и возможностью использования дополнительных средств анонимизации.

Развитие электронных платежных средств связано с внедрением безналичных форм расчетов и банковских карт во второй половине XX века. В дальнейшем с распространением сети Интернет получили развитие системы дистанционного банковского обслуживания, электронные кошельки и мобильные платежные сервисы. В Российской Федерации активное внедрение указанных инструментов началось в 2000-х годах и сопровождалось формированием национальной платежной инфраструктуры.

Правовое регулирование электронных платежных средств осуществляется Федеральным законом от 27.06.2011 № 161-ФЗ «О национальной платежной системе». В соответствии с данным нормативным актом электронное средство платежа представляет собой средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств.

К электронным платежным средствам относятся:

- банковские карты;
- системы интернет-банкинга;
- мобильные платежные приложения;
- электронные кошельки;
- иные технические устройства и технологии, обеспечивающие безналичный перевод денежных средств.

Развитие правового регулирования электронных платежных средств затрагивает и защиту имущественных интересов потерпевших. Федеральным законом от 4 июля 2026 г. № 223-ФЗ статья 29 Гражданского процессуального кодекса Российской Федерации дополнена правилом, позволяющим потерпевшему по уголовному делу о хищении денежных средств с

банковского счета либо электронных денежных средств предъявить иск о взыскании неосновательного обогащения с лица, электронное средство платежа которого использовалось при совершении преступления, а также иск о возмещении имущественного вреда по месту своего жительства или по месту производства уголовного дела. Закон вступает в силу 15 июля 2026 г. Указанная норма непосредственно не регулирует квалификацию легализации, однако расширяет процессуальные возможности восстановления прав потерпевших по предикатным преступлениям, совершаемым с использованием электронных средств платежа¹.

С учетом развития правового режима цифровой валюты и электронных платежных средств особое значение приобретает взаимодействие следственных органов с субъектами финансового мониторинга, кредитными организациями, операторами платежных сервисов, ФНС России и Росфинмониторингом. Именно эти источники позволяют получать сведения о счетах, электронных кошельках, адресах-идентификаторах, времени совершения операций и иных данных, необходимых для реконструкции транзакционной цепочки.

При этом электронные платежные средства сохраняют централизованный характер учета, поскольку информация об операциях фиксируется оператором по переводу денежных средств. Это отличает их от оборота криптовалюты и повышает доказательственное значение банковских выписок, логов доступа, сведений об IP-адресах и данных удаленной идентификации.

Следовательно, при расследовании легализации преступных доходов следователь должен разграничивать правовую природу электронных денежных средств, электронных средств платежа и цифровой валюты,

¹ О внесении изменения в статью 29 Гражданского процессуального кодекса Российской Федерации : Федеральный закон от 04.07.2026 № 223-ФЗ // СПС КонсультантПлюс.

поскольку для каждого из этих инструментов различаются источники доказательственной информации и порядок ее получения.

В отличие от криптовалюты электронные денежные средства имеют централизованный характер учета. Информация о каждой операции фиксируется оператором по переводу денежных средств, что создает возможность последующего получения доказательственной информации в ходе расследования уголовных дел.

Практика показывает, что электронные платежные средства активно используются при реализации схем легализации преступных доходов. Это обусловлено возможностью быстрого перечисления денежных средств между счетами, их дробления, использования номинальных владельцев и проведения многоэтапных финансовых операций, формально не вызывающих подозрения.

В то же время централизованный характер их функционирования позволяет устанавливать маршрут движения денежных средств, круг участников операций и временные параметры совершения транзакций, что имеет важное доказательственное значение.

Таким образом, криптовалюта и электронные платежные средства представляют собой различные по правовой природе финансовые инструменты, использование которых оказывает существенное влияние на механизм совершения и сокрытия легализации преступных доходов.

Если операции с электронными денежными средствами поддаются финансовому контролю и документированию, то оборот криптовалют характеризуется высокой степенью автономности и технологической сложностью, что требует разработки специальных криминалистических рекомендаций по их выявлению и исследованию.

1.3. Криминалистическая классификация легализации денежных средств и иного имущества, совершенной с использованием криптовалюты и электронных платежных средств

Криминалистическая классификация преступлений выступает одним из базовых элементов частной методики расследования, поскольку именно она позволяет систематизировать преступные деяния по признакам, имеющим значение для их выявления, раскрытия и доказывания. В отличие от уголовно-правовой классификации, ориентированной прежде всего на квалификацию содеянного, криминалистическая классификация направлена на выявление закономерностей механизма преступной деятельности, особенностей следообразования, личности преступника и типичных следственных ситуаций.

В криминалистической науке обоснованно отмечается, что классификация преступлений должна строиться с учетом тех признаков, которые определяют выбор тактики следственных действий, специфику взаимодействия с оперативными подразделениями, а также особенности использования специальных знаний. Такой подход позволяет сформировать научно обоснованные рекомендации, ориентированные на практическую деятельность следователя.

Легализация денежных средств и иного имущества, совершенная с использованием криптовалюты и электронных платежных средств, представляет собой сложное многоэтапное деяние, сочетающее признаки преступлений экономической и информационно-технологической направленности. Это обстоятельство обуславливает необходимость ее рассмотрения в рамках нескольких классификационных оснований.

Прежде всего указанные преступления относятся к категории деяний в сфере экономической деятельности, поскольку их конечной целью является придание правомерного вида владению, пользованию и распоряжению имуществом, полученным преступным путем. Вместе с тем использование

цифровых финансовых инструментов придает им выраженный технологический характер, что сближает их с преступлениями, совершаемыми с использованием информационно-телекоммуникационных технологий.

С точки зрения способа совершения легализация преступных доходов с использованием криптовалюты и электронных платежных средств может быть отнесена к числу многоэпизодных преступлений, реализуемых посредством последовательного совершения взаимосвязанных финансовых операций. Каждая из таких операций сама по себе может иметь внешне законный характер, однако в совокупности они образуют единый механизм преступной деятельности, направленный на сокрытие источника происхождения имущества.

В зависимости от характера используемых финансовых инструментов представляется возможным выделить:

- легализацию, осуществляемую преимущественно с использованием криптовалюты;
- легализацию, реализуемую посредством электронных платежных средств;
- смешанные формы, при которых происходит последовательное преобразование денежных средств из безналичной формы в цифровую валюту и обратно.

Последняя разновидность в настоящее время встречается наиболее часто, поскольку позволяет усложнить финансовый след и затруднить его документирование.

По степени организованности преступной деятельности рассматриваемые деяния могут совершаться как отдельными лицами, так и организованными группами. Практика показывает, что наиболее сложные схемы легализации, связанные с использованием цифровых активов, как правило, носят организованный характер и предполагают распределение ролей между участниками. Одни лица обеспечивают получение преступного

дохода, другие — проведение финансовых операций, третьи — создание формальных оснований для придания средствам правомерного вида.

Существенное значение имеет классификация по способу маскировки преступного происхождения имущества. В этой связи могут быть выделены:

- операции, направленные на дробление финансовых потоков;
- многоступенчатые транзакции с использованием различных платежных инструментов;
- конвертация денежных средств в цифровые активы с последующим их переводом между различными адресами;
- использование номинальных владельцев счетов и электронных кошельков;
- применение зарубежных платежных сервисов и криптовалютных платформ.

С точки зрения механизма следообразования данные преступления относятся к числу деяний, характеризующихся преобладанием цифровых следов. Информация о совершенных операциях сохраняется в электронных информационных системах кредитных организаций, платежных сервисов, а также в распределенных реестрах. Это обуславливает необходимость использования специальных знаний в области компьютерной техники, финансового мониторинга и анализа блокчейн-транзакций.

Особое место в классификации рассматриваемых преступлений занимает личность преступника. Для данной категории дел характерно участие лиц, обладающих определенным уровнем финансовой и цифровой грамотности. В ряде случаев преступная деятельность осуществляется с привлечением специалистов в области информационных технологий либо лиц, имеющих опыт работы в финансово-кредитной сфере.

По характеру противоправной деятельности легализация преступных доходов с использованием цифровых финансовых инструментов носит, как правило, латентный характер. Она не сопровождается непосредственным причинением вреда конкретному потерпевшему, а ее выявление становится

возможным в результате финансового мониторинга, оперативно-розыскной деятельности либо расследования предикатного преступления.

Представляется обоснованным рассматривать данные деяния также как преступления с повышенной степенью транснациональности. Использование криптовалютных платформ и зарубежных платежных сервисов позволяет осуществлять финансовые операции вне зависимости от государственной юрисдикции, что существенно осложняет процесс получения доказательственной информации и требует организации международного сотрудничества.

Таким образом, криминалистическая классификация легализации денежных средств и иного имущества, совершенной с использованием криптовалюты и электронных платежных средств, может быть осуществлена по следующим основаниям:

- по сфере преступной деятельности — преступления экономической направленности, совершаемые с использованием информационно-телекоммуникационных технологий;
- по способу совершения — многоэпизодные финансовые операции;
- по используемым инструментам — криптовалюта, электронные платежные средства, их сочетание;
- по степени организованности — индивидуальные и групповые формы;
- по способу сокрытия преступного происхождения имущества;
- по механизму следообразования — преступления с преобладанием цифровых следов;
- по характеру преступной деятельности — латентные, транснациональные.

Выделение указанных классификационных групп имеет не только теоретическое, но и практическое значение. Оно позволяет определить типичные источники доказательственной информации, спрогнозировать следственные ситуации, правильно организовать взаимодействие с

оперативными подразделениями, а также выбрать наиболее эффективные тактические приемы расследования.

Следовательно, криминалистическая классификация выступает методологической основой для построения частной методики расследования легализации преступных доходов, совершенной с использованием криптовалюты и электронных платежных средств, и обеспечивает системный подход к исследованию данного вида преступной деятельности.

Характеристика предикатного преступления. Легализация с использованием криптовалюты и электронных платежных средств практически всегда производна от иного, более тяжкого преступления. Наиболее распространенными предикатами выступают: мошенничество (ст. 159, 159.3, 159.6 УК РФ), незаконный оборот наркотических средств (ст. 228.1 УК РФ), взяточничество (ст. 290 УК РФ) и преступления, совершенные с использованием служебного положения, а также финансирование терроризма и иные преступления террористической направленности. Именно характер предиката предопределяет объем и структуру преступных доходов, а также выбор способа их последующей легализации. Например, по делам о наркопреступлениях чаще используется полная анонимизация через криптовалютные миксеры, а по делам о коррупции — смешанные схемы с частичным выводом через электронные кошельки подконтрольных физических лиц.

Судебная практика подтверждает, что наиболее доказуемыми являются смешанные схемы, в которых цифровая валюта последовательно преобразуется в фиатные денежные средства и поступает на банковские карты либо передается наличными через обменщика. Так, в приговоре Центрального районного суда г. Читы Забайкальского края от 29 августа 2025 г. по делу о легализации доходов, полученных от незаконного оборота наркотических средств, суд указал на получение биткоина на криптовалютный кошелек, последующую продажу криптовалюты через сайт-обменник и зачисление рублей на банковскую карту. Для методики расследования данный пример

важен тем, что показывает типичную цепочку: предикатное преступление — криптовалютный кошелек — онлайн-обменник — банковская карта¹.

Особое значение для данной работы имеет приговор Богучанского районного суда Красноярского края от 27 января 2026 г. по делу № 1-12/2026. Его следует использовать именно как региональный пример из Красноярского края. По делу установлена схема незаконного майнинга: участники размещали оборудование на территории Богучанского района, подключали его к электрическим сетям без договора и учета, добытую криптовалюту аккумулировали на Bybit, затем конвертировали биткоин в USDT и выводили стоимость через посредника в наличные денежные средства и банковские зачисления. При этом в части обвинения по п. «а» ч. 3 ст. 174.1 УК РФ суд оправдал двух подсудимых, поскольку не счел доказанной самостоятельную цель придания правомерного вида владению, пользованию и распоряжению преступным имуществом. Для расследования это означает, что одной лишь конвертации криптовалюты и ее обмена на рубли недостаточно: необходимо доказывать специальную цель легализации, сокрытие происхождения имущества, использование номинальных лиц, фиктивных оснований либо иные действия, направленные именно на введение дохода в легальный оборот.

¹ Приговор Центрального районного суда г. Читы Забайкальского края от 29.08.2025 по делу № 1-125/2025 // СудАкт : [Электронный ресурс]. – URL: <https://sudact.ru/regular/doc/RUuodGTO0411/> (дата обращения: 18.06.2026).

ГЛАВА 2. МЕТОДИКА РАССЛЕДОВАНИЯ ЛЕГАЛИЗАЦИИ ДЕНЕЖНЫХ СРЕДСТВ И ИНОГО ИМУЩЕСТВА, СОВЕРШЕННОЙ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТЫ И ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СРЕДСТВ

2.1. Криминалистическая характеристика легализации денежных средств и иного имущества, совершенной с использованием криптовалюты и электронных платежных средств

Криминалистическая характеристика преступлений выступает в качестве информационной основы для построения частных методик расследования, аккумулируя в себе данные о типичных признаках и закономерностях механизма совершения конкретного вида деяний. Для легализации денежных средств и иного имущества, совершаемой с использованием криптовалюты и электронных платежных средств, такая характеристика имеет принципиальное значение, поскольку цифровая природа данных финансовых инструментов предопределяет специфику способов совершения, обстановки, личности преступника и механизма следообразования.

Как обоснованно отмечает профессор Р.С. Белкин, криминалистическая характеристика позволяет перейти от общего понятия преступной деятельности к частным рекомендациям по ее выявлению и раскрытию. Применительно к исследуемой категории уголовных дел элементы криминалистической характеристики обладают существенными особенностями, отличающими их от традиционных преступлений в сфере экономической деятельности. Криминалистическая характеристика преступления – вероятностная модель события и как таковая может быть основанием для вероятностных же умозаключений – следственных версий.

Криминалистическая характеристика на конкретный случай позволяет построить его вероятностную модель. Именно в этом и заключается ее практическое значение, которое не следует преувеличивать, поскольку содержащееся в криминалистической характеристике знание носит не достоверный, а вероятностный характер. Но на начальном этапе расследования всякое истинное знание, даже вероятное, имеет высокую цену, поскольку позволяет следователю снизить информационную неопределенность¹.

Способ совершения преступления является центральным элементом криминалистической характеристики. Можно выделить три типичные группы способов легализации с использованием цифровых финансовых инструментов.

Первую группу составляют способы, основанные на конверсии преступных доходов через криптовалюту. Преступные денежные средства (наличные или безналичные) направляются на приобретение цифровой валюты (как правило, Bitcoin, Ethereum) через обменные пункты (как легальные биржи, так и нелегальные P2P-платформы, не осуществляющие идентификацию клиентов). Затем криптовалюта подвергается процедуре «микширования» (tumbler, mixer) — смешиванию с транзакциями других пользователей, что разрывает финансовый след. После этого «очищенная» криптовалюта обменивается обратно на фиатные деньги, которые уже поступают на подконтрольные счета как средства от законной деятельности (продажа цифровых активов, инвестиции)².

Вторая группа связана с использованием электронных платежных средств. Здесь типичным является дробление крупных сумм на множество микротранзакций (структурирование), перевод средств между большим

¹ Белкин Р.С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики : монография. – М. : Норма-Инфра, 2001. – 240 с.

² Жамбалов, Д.Б. Криминалистическая характеристика легализации (отмывания) доходов, полученных преступным путем / Д.Б. Жамбалов // Вестник Восточно-Сибирского института МВД России. – 2019. – № 4 (91). – С. 159–168.

количеством номинальных счетов (дропов), а также использование электронных кошельков (Qiwi, YooMoney, WebMoney), зарегистрированных на подставных лиц или по утерянным документам. Завершающим этапом нередко становится обналичивание через подконтрольные организации-однодневки или вывод средств за рубеж с использованием систем денежных переводов.

Третья, наиболее сложная группа — смешанные способы, сочетающие криптовалюту и электронные платежные средства. Такая многоступенчатость направлена на максимальное усложнение документирования преступной деятельности.

Обстановка совершения преступления характеризуется использованием распределенной инфраструктуры. Временной фактор практически не ограничен, операции могут совершаться круглосуточно из любой точки мира. Пространственная характеристика включает как виртуальную среду (блокчейн-сети, сайты обменников), так и физические места доступа (компьютеры, мобильные устройства с выходом в сеть Интернет). Важной особенностью является трансграничность: серверы криптобирж могут находиться в одной юрисдикции, а операторы электронных кошельков — в другой, а сам преступник — в третьей.

Местом преступления будет являться место расположения устройства, с помощью которого совершены противоправные действия, связанные с легализацией. В качестве таковых могут использоваться любые технически сложные устройства: персональные компьютеры, ноутбуки, планшеты, смартфоны и иные ЭВМ, располагающие функционалом по выполнению подобного рода операций – действий на сайтах или в приложениях бирж или криптообменников, вычислительная сложность которых не превышает сложность действий на информационном сайте, открытом через браузер¹.

¹ Корноухов, В.Е. Курс криминалистики. Особенная часть. Т. 2. Методики расследований преступлений в сфере экономики, охраны труда, пожарной безопасности, экологии и транспорта / отв. ред. В.Е. Корноухов. – М. : Юрист, 2004. – 541 с.

В ситуациях, когда установить точное место совершения противоправных операций по легализации денежных средств с использованием криптовалюты затруднительно, оправданным является задействование механизмов международного взаимодействия. Речь идет о направлении мотивированных запросов иностранным криптобиржам, операторам сервисов, предоставляющих инфраструктуру криптовалютных кошельков, а также об обращении в правоохранительные органы зарубежных государств. Вместе с тем санкционная политика ряда иностранных государств в отношении Российской Федерации существенно осложняет такое взаимодействие: помощь российским правоохранительным органам со стороны зарубежных коллег может быть ограниченной либо полностью отсутствовать.

Специфика обстановки при использовании электронных платежных средств имеет иной характер, хотя сохраняет ряд общих черт с криптовалютой. Электронные платежные средства (банковские карты, системы интернет-банкинга, электронные кошельки, а также мобильные платежные приложения) функционируют в централизованной, а не распределенной среде. Это означает, что у каждой операции есть конкретный оператор (банк или небанковская кредитная организация), который обязан хранить сведения об операциях и предоставлять их правоохранительным органам в установленном законом порядке. Поэтому «виртуальная» составляющая обстановки здесь выражена слабее, чем при обороте криптовалюты, зато существенно возрастает значение документарных и учетных данных.

Временной фактор при использовании электронных платежных систем также практически не ограничен — операции могут проводиться круглосуточно, выходные и праздники не являются препятствием. Пространственная характеристика включает личный кабинет в системе интернет-банка, мобильное приложение, терминал самообслуживания

(банкомат или платежный терминал), а также физическое местонахождение самого плательщика.

Предметом легализации, как следует из норм уголовного закона, являются денежные средства и иное имущество. При этом, исходя из анализа следственной практики, денежные средства в качестве предмета преступления встречаются значительно чаще, чем иное имущество. Кроме того, денежные средства используются во всех рассмотренных схемах отмыывания, т.е. при двухфазовой, трехфазовой и четырехфазовой моделях легализации. Во всех отмеченных схемах в зависимости от конкретного способа легализации они могут быть представлены как в наличной форме, так и в безналичной, т.е. находящиеся на счетах физических и юридических лиц в финансовых учреждениях. Кроме того, денежные средства могут быть представлены как в национальной валюте, так и в иностранной¹. В качестве обязательного признака предмета легализации выделяется источник его происхождения, а именно происхождение в результате совершения конкретного преступления, доказывание которого является прерогативой следственных органов в рамках расследования предикатного состава преступления. С учетом Федерального закона от 20.02.2026 № 38-ФЗ цифровая валюта признается имуществом для целей УК РФ и УПК РФ. Следовательно, по делам о легализации предметом преступления могут выступать как денежные средства, преобразованные из цифровой валюты, так и сама цифровая валюта, если она получена преступным путем либо используется для придания правомерного вида преступным доходам.

Личность преступника по данной категории дел, как правило, не совпадает с типичным портретом традиционного «отмывателя» денег. Исходя

¹ Вильская, Н.В. О некоторых особенностях криминалистической характеристики преступлений, совершенных с использованием криптовалюты / Н.В. Вильская, В.Ю. Малахова // Проблемы экономики и юридической практики. – 2024. – № 1. – С. 94–101.

из анализа эмпирических данных и научных трудов (в частности, В.Е. Корноухова¹), можно выделить две основные категории:

Профессиональные участники: лица с высшим экономическим или техническим (ИТ) образованием, владеющие навыками работы с блокчейном, криптобиржами и анонимизирующими сервисами. Нередко имеют опыт легальной деятельности в сфере финансовых технологий. Их мотив — получение систематического дохода от оказания «услуг» по выводу средств для организованных преступных групп.

«Дропы» и номинальные держатели: лица, часто с низким социальным статусом, студенты или граждане с зависимостями, которые за материальное вознаграждение предоставляют свои паспортные данные для регистрации электронных кошельков или проходят процедуры идентификации на биржах. В уголовно-правовом смысле они могут выступать как соучастники, однако зачастую сами не осознают полной картины преступной схемы.

Для организаторов характерны такие качества, как высокая адаптивность к изменениям законодательства, использование средств криптографической защиты переписки, а также стремление минимизировать свой цифровой след.

Личность преступника при легализации денежных средств с использованием криптовалюты имеет ряд отличительных черт, которые во многом предопределены самой природой цифровых финансовых инструментов. Если сопоставить возрастные характеристики лиц, совершающих такие преступления, с теми, кто занимается аналогичной противоправной деятельностью, но без применения криптовалюты, можно заметить вполне определенную специфику.

¹ Корноухов В.Е. Курс криминалистики. Особенная часть. Т. 2. Методики расследований преступлений в сфере экономики, охраны труда, пожарной безопасности, экологии и транспорта / отв. ред. В.Е. Корноухов. – М. : Юрист, 2004. – 541 с.

Прежде всего обращает на себя внимание сравнительно молодой возраст фигурантов. Средний показатель здесь колеблется в диапазоне от 18 до 26 лет. При этом доля несовершеннолетних среди данной категории преступников также выше, чем в других составах экономической направленности. С чем это связано? По всей видимости, с тем, что наиболее активная аудитория пользователей сети Интернет — это как раз молодежь. Молодые люди в возрасте до 30 лет составляют практически половину от всех, кто регулярно пользуется глобальной сетью. Соответственно, и криминальная активность в цифровой среде неизбежно «молодеет».

Если обобщить позиции большинства исследователей, занимавшихся данной проблематикой, то возрастной диапазон лиц, совершающих преступления в киберпространстве, можно обозначить интервалом от 15 до 45 лет. Что касается социального положения — здесь разброс очень широкий: от школьника или студента до вполне взрослого сотрудника государственного органа или коммерческой структуры¹.

Не менее интересная картина складывается с полом преступника. Если взять для сравнения традиционные (нецифровые) способы легализации, то там соотношение мужчин и женщин не столь разительно. В случае же с использованием криптовалюты доля мужчин становится подавляющей. По разным оценкам, она составляет от 89 до 98 процентов². Объяснений здесь может быть несколько: и специфика технической подготовки, и особенности поведения в виртуальной среде, и, возможно, просто сложившийся «портрет» криптоинвестора или трейдера, среди которых мужчин традиционно больше.

Еще одна характерная черта — большинство таких преступников не состоят в браке. Причины тут двоякие. С одной стороны, сказывается молодой

¹ Кесарева Г.Ю. Криминалистическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет : дис. ... канд. юрид. наук. – М., 2002. – С. 101–105.

² Вильская Н.В., Малахова В.Ю. О некоторых особенностях криминалистической характеристики преступлений, совершенных с использованием криптовалюты // Проблемы экономики и юридической практики. – 2024. – № 1. – С. 94–101.

возраст фигурантов — они просто еще не успели создать семью. С другой — есть и чисто прагматический момент: женатые люди, особенно имеющие детей, чаще опасаются, что их противоправная деятельность может негативно отразиться на близких. Поэтому они либо вообще не идут на такой риск, либо действуют гораздо осторожнее, что снижает их выявляемость. А вот молодые, холостые, не обремененные семейными обязательствами, зачастую относятся к риску легкомысленнее, что и делает их основной «целевой аудиторией» для вовлечения в схемы с криптовалютой.

Механизм слеδοобразования имеет ярко выраженный цифровой характер. Традиционные материальные следы (отпечатки пальцев, следы обуви) на месте преступления либо отсутствуют, либо не имеют решающего значения. Основной объем доказательственной информации содержится в цифровых следах, которые можно классифицировать на:

Следы в блокчейне: записи о транзакциях (хэши, адреса кошельков отправителя и получателя, временные метки, суммы), которые хранятся в распределенном реестре и не могут быть ретроспективно изменены.

Следы у операторов электронной платежной системы и банков: логи операций, IP-адреса устройств, с которых осуществлялся доступ, биометрические данные при удаленной идентификации.

Следы на устройствах пользователей: файлы cookie, история браузера, сохраненные пароли, криптокошельки в приложениях, файлы конфигурации обменных сервисов.

Коммуникационные следы: переписка в мессенджерах (Telegram, Signal) относительно условий обмена, кошельков и реквизитов.

Важной особенностью является высокая степень сохранности, но одновременно и хрупкость цифровых следов: данные могут быть зашифрованы, удалены или находиться на серверах за пределами РФ, что требует неотложного производства следственных действий, направленных на их фиксацию (осмотр предметов и документов, выемка, получение информации о соединениях).

Характеристика предикатного преступления. Легализация с использованием криптовалюты и электронных платежных средств практически всегда производна от иного, более тяжкого преступления. Наиболее распространенными предикатами выступают: мошенничество (ст. 159, 159.3, 159.6 УК РФ), незаконный оборот наркотических средств (ст. 228.1 УК РФ), взяточничество (ст. 290 УК РФ) и преступления, совершенные с использованием служебного положения, а также финансирование терроризма и иные преступления террористической направленности. Именно характер предиката предопределяет объем и структуру преступных доходов, а также выбор способа их последующей легализации. Например, по делам о наркопреступлениях чаще используется полная анонимизация через криптовалютные миксеры, а по делам о коррупции — смешанные схемы с частичным выводом через электронные кошельки подконтрольных физических лиц.

Обобщая изложенное, следует заключить, что криминалистическая характеристика легализации денежных средств и иного имущества, совершенной с использованием криптовалюты и электронных платежных средств, включает следующие взаимосвязанные элементы: способы совершения (конверсия через криптовалюту, использование электронных платежных средств, смешанные схемы); обстановку (виртуальная трансграничная среда); предмет; личность преступника (профессиональные участники и «дропы»); механизм цифрового слеодообразования (следы в блокчейне, у операторов, на устройствах); а также связь с предикатным преступлением. Понимание данных элементов позволяет следователю уже на этапе возбуждения уголовного дела определить направления первоначальных следственных действий, круг подлежащих допросу лиц и необходимые специальные знания, что в конечном итоге повышает эффективность раскрытия и расследования данной категории преступлений в условиях цифровой трансформации экономических отношений.

2.2. Типичные следственные ситуации легализации денежных средств и иного имущества, совершенной с использованием криптовалюты и электронных платежных средств

Практика расследования преступлений, предусмотренных статьями 174 и 174.1 Уголовного кодекса Российской Федерации, показывает, что каждая конкретная проверка или уголовное дело в этой сфере разворачиваются в уникальных обстоятельствах. Однако при всем многообразии ситуаций, с которыми сталкивается следователь, существует ряд повторяющихся, наиболее характерных комбинаций обстоятельств, имеющих значение для выдвижения версий, планирования расследования и выбора тактических приемов. В криминалистической методике такие комбинации принято называть типичными следственными ситуациями.

По мнению профессора А.Г. Филиппова, типология следственных ситуаций должна строиться на двух ключевых параметрах: во-первых, на степени информационной определенности, во-вторых, на том, какие источники доказательственной информации уже имеются в распоряжении следователя к моменту принятия решения о возбуждении уголовного дела либо непосредственно после этого. Применительно к легализации доходов с использованием криптовалюты и электронных платежных средств этот подход требует определенной корректировки в силу специфики цифрового следа¹.

Можно выделить четыре наиболее часто встречающиеся типичные следственные ситуации.

¹ Криминалистика : учебник для вузов / под ред. А.Г. Филиппова. – 3-е изд., перераб. и доп. – М. : Издательство Юрайт, 2025. – 402 с.

Ситуация первая: поступление первичной информации от подразделения финансового мониторинга (Росфинмониторинг).

Данная ситуация возникает, когда в правоохранительные органы направляются сведения о сомнительных финансовых операциях. В соответствии с Федеральным законом от 07.08.2001 № 115-ФЗ организации, осуществляющие операции с денежными средствами или иным имуществом (в том числе кредитные организации, операторы электронных денежных средств и иные субъекты первичного финансового мониторинга), обязаны выявлять операции, имеющие признаки необычных или подозрительных. В отношении цифровой валюты информация может поступать также через сведения ФНС России о майнинге и адресах-идентификаторах, материалы Росфинмониторинга, данные операторов цифровых финансовых активов и сведения, полученные в рамках экспериментальных правовых режимов. Поэтому некорректно сводить такую информацию к «криптобиржам, прошедшим регистрацию в РФ»¹.

На момент получения такой информации у следователя, как правило, нет данных о том, какое именно предикатное преступление послужило источником легализуемых средств. Имеются лишь формальные признаки: объемы, участники, время совершения операций. Информационная определенность здесь оценивается как низкая либо средняя. Главная задача в этой ситуации — не возбуждать уголовное дело «вслепую», а организовать доследственную проверку в порядке статей 144-145 УПК РФ, в ходе которой необходимо направить запросы в кредитные организации для получения расширенных выписок, а также навести справки об участниках операций через оперативные учеты.

Ситуация вторая: выявление легализации в рамках расследования предикатного преступления.

¹ О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма : Федеральный закон от 07.08.2001 № 115-ФЗ // СПС КонсультантПлюс.

Это, пожалуй, самая распространенная ситуация в практике подразделений по расследованию экономических преступлений. Следователь ведет уголовное дело, скажем, по факту мошенничества в крупном размере (ч. 4 ст. 159 УК РФ) или получения взятки (ст. 290 УК РФ). В ходе допросов обвиняемых, выемки документов, анализа выписок по счетам он обнаруживает, что похищенные или полученные незаконным путем денежные средства не просто присвоены или истрачены на личные нужды, а подверглись процедуре «очистки»: часть средств была переведена на электронные кошельки номинальных держателей, затем конвертирована в криптовалюту через P2P-обменник, после чего — обналичены за рубежом либо использована для приобретения дорогостоящего имущества, оформленного на подставных лиц.

В отличие от предыдущей ситуации, здесь у следователя уже есть лицо, подозреваемое в совершении предикатного преступления, и часть доказательств его вины. Однако легализационный эпизод требует самостоятельного доказывания, поскольку состав преступления по ст. 174.1 УК РФ (легализация собственных доходов) не поглощается составом предиката. Информационная определенность в этой ситуации может быть высокой, если в ходе обыска изъяты электронные носители с паролями от криптокошельков, либо низкой, если обвиняемый уничтожил цифровые следы. Типичные действия: назначение компьютерной судебной экспертизы изъятых устройств, допрос обвиняемого о схемах вывода средств (здесь важно использовать тактический прием «дробления» — детализировать каждую операцию), а также наложение ареста на обнаруженную цифровую валюту в порядке ст. 115 УПК РФ с учетом специальных правил, введенных Федеральным законом от 20.02.2026 № 38-ФЗ.

Именно к этой ситуации относится рассмотренное Богучанским районным судом Красноярского края дело о незаконном майнинге: легализационный эпизод был выявлен не изолированно, а через расследование предикатных действий, связанных с причинением имущественного ущерба

энергоснабжающей организации и коррупционным поведением должностного лица. Практический вывод состоит в том, что следователь должен планировать доказывание по двум уровням: сначала установить преступное происхождение цифровой валюты, затем отдельно доказать, что последующие операции с ней были направлены не просто на расходование дохода, а на придание ему правомерного вида.

Ситуация третья: оперативная информация о деятельности организованной группы, специализирующейся на «отмыве» денег через криптобиржи.

Эта ситуация характеризуется высоким уровнем латентности и, как правило, инициируется материалами, полученными в результате оперативно-розыскной деятельности сотрудниками подразделений экономической безопасности и противодействия коррупции (ЭБиПК) либо подразделениями по борьбе с киберпреступностью. Из рапорта и справки-меморандума следует, что группа лиц (нередко с IT-образованием) на постоянной основе оказывает услуги по выводу и консервации преступных доходов с использованием криптовалютных миксеров и зарубежных бирж, не требующих верификации.

На момент возбуждения уголовного дела следователь располагает данными о лицах — организаторах схемы, о примерных объемах обналичиваемых средств, но не знает конкретных предикатных преступлений, доходы от которых легализуются. Это осложняет квалификацию по ст. 174 УК РФ (поскольку для доказывания нужен факт заведомости о преступном происхождении средств от других лиц). Выходом из этой ситуации является возбуждение уголовного дела по ст. 172 УК РФ (незаконная банковская деятельность) или ст. 210 УК РФ (организация преступного сообщества) с последующим выделением эпизодов легализации по мере установления источников средств.

Основная сложность здесь — скоротечность. Получив информацию о том, что их схема раскрыта, участники группы мгновенно закрывают «кошельки», переходят на новые биржи и уничтожают электронные

устройства. Поэтому тактически верным решением будет проведение массированного одновременного обыска с привлечением специалистов в области информационных технологий для изъятия и оперативного исследования оборудования.

По такой логике может анализироваться приговор Останкинского районного суда г. Москвы от 11 августа 2025 г., где в материалах дела отражены операции через несколько обменных сервисов, многочисленные обменные заявки и криптовалютные адреса с установленным количеством транзакций. Этот пример показывает, что при расследовании организованной цифровой схемы следователь должен не ограничиваться одним кошельком, а устанавливать всю инфраструктуру: используемые обменники, адреса, заявки, банковские карты, устройства и аккаунты, через которые осуществлялся доступ¹.

Ситуация четвертая: заявление потерпевшего о том, что его денежные средства были похищены и впоследствии «отмыты» через обменники криптовалют.

В качестве реального примера можно использовать приговор Центрального районного суда г. Читы Забайкальского края от 29 августа 2025 г.: суд установил, что лицо получало преступный доход в виде биткоина, использовало криптовалютный кошелек, затем через сайт-обменник uxbtc.pro продало цифровую валюту, а рублевый эквивалент был зачислен на банковскую карту. Для следователя в такой ситуации ключевыми источниками становятся сведения о кошельке, обменнике, банковской карте, IP-адресах входа, переписке с обменщиком и связи этих операций с предикатным преступлением².

¹ Приговор Останкинского районного суда г. Москвы от 11.08.2025 по делу № 01-0570/2025 // СудАкт : [Электронный ресурс]. – URL: <https://sudact.ru/regular/doc/jd9OqWoMBA1r/> (дата обращения: 18.06.2026).

² Приговор Центрального районного суда г. Читы Забайкальского края от 29.08.2025 по делу № 1-125/2025 // СудАкт : [Электронный ресурс]. – URL: <https://sudact.ru/regular/doc/RUuodGTO0411/> (дата обращения: 18.06.2026).

На момент проверки у следователя есть заявитель, есть адреса криптокошельков (если потерпевший сохранил скриншоты или историю операций), но нет лица, совершившего преступление. Оперативно установить его крайне сложно, так как криптобиржи зачастую расположены в юрисдикциях, не сотрудничающих с российскими правоохранительными органами (например, в отдельных офшорных зонах). Типичная ошибка в этой ситуации — отказ в возбуждении уголовного дела со ссылкой на невозможность установить лицо. Правильный алгоритм: возбуждать уголовное дело по факту мошенничества (ст. 159 УК РФ) и одновременно давать поручение органу дознания о направлении международных следственных поручений в компетентные органы государства регистрации криптобиржи. Параллельно следователь должен назначить судебную компьютерно-техническую экспертизу для анализа движения средств по блокчейну с привлечением специализированного программного обеспечения.

Обобщая изложенное, следует подчеркнуть, что каждая из рассмотренных типичных следственных ситуаций требует от следователя дифференцированного подхода. В первой ситуации приоритетом является грамотная доследственная проверка с запросами в Росфинмониторинг. Во второй — неотложное производство обысков и выемок электронных носителей, а также допросы с детализацией финансовых операций. В третьей ситуации — межведомственное взаимодействие и силовые оперативно-следственные мероприятия. В четвертой — быстрое возбуждение дела и использование возможностей международного сотрудничества, пусть даже с ограниченным результатом.

Важно понимать, что на практике эти ситуации редко встречаются в чистом виде. Нередко следователь сталкивается с комбинированными вариантами, когда первичная информация от финансового мониторинга накладывается на уже расследуемое предикатное преступление.

2.3. Система тактических задач и способы их решения легализации денежных средств и иного имущества, совершенной с использованием криптовалюты и электронных платежных средств

Любая криминалистическая методика была бы неполной без четкого представления о том, какие именно задачи приходится решать следователю на разных этапах расследования. Применительно к легализации преступных доходов с использованием цифровых финансовых инструментов система тактических задач имеет свои особенности. Они обусловлены тем, что классическая триада «обнаружить — зафиксировать — изъять» работает здесь не в полной мере, поскольку доказательства существуют преимущественно в виртуальной среде и требуют специфических приемов работы.

В криминалистической литературе, в частности в работах профессора В.Е. Корноухова, обоснованно отмечается, что тактическая задача представляет собой конкретную цель, достижение которой обеспечивает продвижение по делу в условиях определенной следственной ситуации. Применительно к нашей теме такие задачи можно разделить на три уровня: общие (характерные для всех экономических преступлений), специальные (связанные с особенностями легализации) и частные (обусловленные использованием криптовалюты и электронных платежных средств). Наибольший интерес представляют последние две группы.

Первая группа тактических задач: информационно-поисковые.

Их суть заключается в обнаружении источников сведений о движении преступных доходов. В отличие от традиционных хищений, где есть материальный ущерб и конкретный потерпевший, при легализации такового может не быть вовсе, либо он «размыт» по множеству номинальных счетов.

Способами решения здесь выступают:

Во-первых, своевременное направление запросов в Управление Росфинмониторинга. Эти сведения позволяют установить транзакционную цепочку — от первого поступления средств на подконтрольный счет до попытки их конвертации в криптовалюту или вывода за рубеж. Запрос должен быть сформулирован максимально конкретно: с указанием периодов, сумм (даже приблизительных), реквизитов счетов и паспортных данных фигурантов.

Во-вторых, получение информации о соединениях между абонентами и (или) абонентскими устройствами в порядке ст. 186.1 УПК РФ. Здесь важно понимать: лица, занимающиеся легализацией через криптовалюту, редко используют обычную голосовую связь. Чаще это мессенджеры (Telegram, WhatsApp). Однако сам факт соединения с определенными IP-адресами, с которых осуществлялся вход на криптобиржу или в электронный кошелек, может стать отправной точкой для установления местонахождения преступника или используемых им устройств.

В-третьих, взаимодействие с подразделением БСТМ ГУ МВД России. Сотрудники этого подразделения обладают компетенциями по поиску и фиксации цифровых следов в открытых и закрытых сегментах сети Интернет, включая даркнет-площадки, где нередко заказываются услуги по обналаживанию через криптомиксеры. Следовательно не нужно самому погружаться в технические детали — достаточно грамотно поставить задачу в письменном поручении.

В-четвертых, при анализе криптовалютных операций целесообразно использовать специализированные аналитические инструменты блокчейн-аналитики. В частности, Росфинмониторинг указывает, что программа для ЭВМ «Прозрачный блокчейн. Государственный модуль» предназначена для мониторинга криптовалютных транзакций, анализа финансовых потоков в криптовалюте и проведения расследований в сфере обращения криптовалют в целях противодействия отмыванию доходов, финансированию терроризма и распространению оружия массового уничтожения. Такие инструменты не

заменяют процессуального доказывания, однако позволяют быстрее выявлять транзакционные цепочки, связанные адреса и признаки использования сервисов сокрытия следа¹.

Практическое значение такой задачи видно на примере указанного приговора Останкинского районного суда г. Москвы: в деле исследовались данные нескольких обменных сервисов, сведения о десятках и сотнях обменных операций, а также криптовалютные адреса с установленной историей транзакций. Поэтому информационно-поисковая задача должна включать не только запросы в банки, но и фиксацию хэшей, адресов-идентификаторов, заявок обменника, аккаунтов в мессенджерах и устройств, с которых оформлялись операции.

Вторая группа тактических задач: обеспечительные и охранительные.

Здесь речь идет о предотвращении возможности скрыть или уничтожить цифровые доказательства, а также о наложении ареста на обнаруженные активы.

Особое значение имеет обеспечительная тактическая задача, связанная с наложением ареста на цифровую валюту и ее изъятием. Ранее данный вопрос оставался одним из наиболее проблемных в следственной практике, поскольку УПК РФ не содержал специальных правил обращения с цифровой валютой. После принятия Федерального закона от 20.02.2026 № 38-ФЗ цифровая валюта прямо признается имуществом для целей УК РФ и УПК РФ, а уголовно-процессуальное законодательство предусматривает специальные правила ее изъятия, хранения и ареста.

При решении обеспечительных задач следует учитывать Информационное письмо Росфинмониторинга от 19 июня 2026 г. № 69, содержащее методические рекомендации по применению субъектами

¹ Программа для ЭВМ «Прозрачный блокчейн. Государственный модуль» // Росфинмониторинг : [Электронный ресурс]. – URL: <https://www.fedsfm.ru/activity/informational-systems/pb-gos-modul> (дата обращения: 18.06.2026).

Федерального закона № 115-ФЗ мер по замораживанию (блокированию) денежных средств или иного имущества, снятию таких мер и приостановлению операций. Эти рекомендации ориентированы прежде всего на субъектов первичного финансового мониторинга, однако имеют значение и для организации взаимодействия следователя с кредитными и иными обязанными организациями: они позволяют уточнить, какие ограничительные меры применялись к активам, когда они вводились или отменялись и какие сведения передавались в Росфинмониторинг. Полученная информация может использоваться для проверки транзакционной цепочки и своевременного принятия процессуальных мер по сохранению имущества¹.

Изъятие цифровой валюты, а также материальных носителей, на которых она хранится или на которых зафиксированы сведения, обеспечивающие доступ к ней, должно осуществляться с участием специалиста. Материальный носитель подлежит изъятию и хранению в опечатанном виде в условиях, исключающих доступ посторонних лиц к закрытым ключам, seed-фразам, паролям и иным данным доступа. При наложении ареста, если имеется техническая возможность, цифровая валюта может переводиться на адрес-идентификатор для обеспечения ее сохранности.

В связи с этим тактически правильным является не формальное изъятие телефона или компьютера, а заранее подготовленное следственное действие с участием специалиста в сфере информационных технологий и блокчейн-аналитики. Следователь должен обеспечить фиксацию устройства, кошелька, адреса-идентификатора, обнаруженных данных доступа и последовательности действий специалиста, поскольку нарушение порядка фиксации может повлечь споры о допустимости доказательств.

¹ Информационное письмо от 19.06.2026 № 69 «Методические рекомендации по применению субъектами исполнения Федерального закона от 07.08.2001 № 115-ФЗ мер по замораживанию (блокированию) денежных средств или иного имущества и снятию таких мер, а также приостановлению операций с денежными средствами или иным имуществом» // СПС КонсультантПлюс

С учетом обновленного правового режима майнинга отдельной обеспечительной задачей является проверка, имелись ли у лица сведения в реестре майнеров, договор с сетевой или энергоснабжающей организацией, а также представлялись ли в ФНС России сведения о получении цифровой валюты и адресах-идентификаторах. Отсутствие таких данных само по себе не доказывает легализацию, но помогает подтвердить незаконный характер получения цифровой валюты и сформировать версию о ее преступном происхождении.

Способом решения обеспечительной задачи выступает также применение меры пресечения в виде домашнего ареста либо запрета определенных действий, в частности запрета пользоваться сетью Интернет. Несмотря на трудности контроля, такое ограничение создает дополнительные правовые последствия для подозреваемого и позволяет впоследствии обосновать ходатайство об изменении меры пресечения на более строгую при попытке уничтожения цифровых следов или перевода цифровых активов.

Третья группа тактических задач: доказывание объективной стороны преступления.

Суть данной группы задач — в придании доказательственного значения сведениям, полученным из цифровых источников. Проблема в том, что скриншот экрана с адресом криптокошелька или историей транзакций, сделанный самим следователем, в суде часто оспаривается защитой со ссылкой на возможность монтажа.

Надежным способом решения является производство осмотра предметов и документов с участием специалиста и с применением средств видеозаписи. В протоколе осмотра электронного устройства или страницы сайта криптообменника необходимо детально описывать не только то, что видно на экране, но и последовательность действий следователя (какой браузер открыт, по какому адресу осуществлен переход, какие кнопки нажаты). Дополнительно следует изымать не сам скриншот, а исходные

данные — к примеру, файл кэша браузера или дампы оперативной памяти компьютера, который впоследствии исследует эксперт.

В приговоре Городищенского районного суда Волгоградской области от 2 июня 2025 г. доказательственное значение имели показания специалиста о механизме работы криптовалюты, онлайн-обменников, переводе цифрового актива в рубли и зачислении средств на банковские карты. Данный пример показывает, что специалист нужен не формально, а для объяснения суду технической логики операции: каким образом цифровая валюта превращается в рубли, где разрывается связь между первоначальным источником средств и конечным получателем, какие цифровые следы остаются после обмена¹.

Четвертая группа тактических задач: организационно-управленческие.

Они связаны с необходимостью взаимодействия между разными субъектами расследования. Легализация через криптовалюту и электронные платежные средства — это не то дело, которое следователь может раскрыть в одиночку, работая только с документами.

Способами решения здесь выступают:

Планирование одновременных следственных действий. Если по делу проходит несколько фигурантов, проживающих в разных районах города (к примеру, Красноярска, Дивногорска и Сосновоборска), обыски у них должны проводиться в один и тот же час, чтобы не допустить утечки информации через мессенджеры.

Использование возможностей международно-правового сотрудничества. Это, пожалуй, самая сложная организационная задача, поскольку направление международного следственного поручения в компетентный орган другого государства (к примеру, на Кипр или в Эстонию, где зарегистрированы многие криптобиржи) требует времени и грамотного

¹ Приговор Городищенского районного суда Волгоградской области от 02.06.2025 по делу № 1-140/2025 // СудАкт : [Электронный ресурс]. – URL: <https://sudact.ru/regular/doc/NgxoeUAjH7b8/> (дата обращения: 18.06.2026).

юридического оформления. Однако без этого невозможно получить информацию от зарубежных операторов, не имеющих представительств в РФ.

О способах решения ситуативных задач на первоначальном этапе.

Применительно к расследованию легализации с использованием цифровых инструментов можно выделить несколько тактических приемов, доказавших свою эффективность на практике:

Прием «цифрового двойника». Суть в том, что следователь, получив данные о транзакции через один блокчейн-обозреватель, проверяет их через другой, независимый сервис. Совпадение сведений снимает возражения защиты о возможной технической ошибке.

Прием «последовательной детализации». На допросе подозреваемого не следует спрашивать абстрактно: «Куда вы дели деньги?». Вопросы задаются подробно, по каждой операции: «С какого устройства вы зашли на биржу?», «Какой адрес кошелька получателя вы скопировали?», «Какую комиссию заплатили за транзакцию?». Невозможность ответить на детальные вопросы при наличии общего признания вины — серьезный аргумент для суда.

Прием «отложенного обыска» применяется в ситуациях, когда есть основания полагать, что фигурант хранит закрытые ключи от криптокошелька не дома, а в ином месте (к примеру, в арендованной ячейке банка или у доверенного лица). В этом случае сначала проводится наблюдение, затем — одновременный обыск по всем возможным адресам. Риск заключается в том, что преступник может удаленно перевести средства, узнав об интересе к нему. Поэтому такой прием оправдан только при наличии данных о том, что физический доступ к устройству с кошельком ограничен.

Отдельной тактической задачей является доказывание специальной цели легализации. Апелляционная практика показывает, что суды внимательно проверяют, установлены ли конкретные фактические обстоятельства, свидетельствующие о придании правомерного вида преступным доходам. Поэтому в обвинении и доказательственной базе необходимо не ограничиваться общей формулой «конвертировал криптовалюту в рубли», а

раскрывать, какие именно действия свидетельствовали о сокрытии происхождения имущества и обеспечении его дальнейшего свободного оборота¹.

В завершение следует подчеркнуть, что система тактических задач при расследовании легализации с использованием криптовалюты и электронных платежных средств не является раз и навсегда заданной. Она меняется в зависимости от следственной ситуации, технической оснащенности следователя и уровня цифровой грамотности противодействующей стороны. Тем не менее это позволяет структурировать работу, избежать хаотичности в проведении следственных действий и, что самое важное, не упустить момент, когда цифровые доказательства еще можно сохранить.

2.4. Криминалистические особенности легализации денежных средств и иного имущества, совершенной с использованием криптовалюты и электронных платежных средств

Когда речь заходит о расследовании легализации преступных доходов с применением цифровых финансовых инструментов, традиционные криминалистические рекомендации, разработанные еще в конце прошлого века для борьбы с «обычным» отмыванием денег через банки и подставные фирмы, работают далеко не всегда. Появились обстоятельства, которые раньше либо отсутствовали вовсе, либо не имели решающего значения, а сегодня выходят на первый план. Эти обстоятельства в криминалистике принято называть особенностями расследования. Их знание позволяет

¹ Апелляционное постановление Ярославского областного суда от 20.04.2025 по делу № 1-51/2025 // СудАкт : [Электронный ресурс]. – URL: <https://sudact.ru/regular/doc/wkmsreIoJFQ3/> (дата обращения: 18.06.2026).

следователю не действовать методом проб и ошибок, а сразу выбирать наиболее эффективные тактические решения.

Можно выделить следующие основные криминалистические особенности, отличающие данную категорию преступлений от легализации, совершаемой традиционными способами.

Первая особенность: доминирование цифровых следов над материальными.

При расследовании обычного хищения следователь ищет следы рук, обуви, орудий взлома, видеозаписи с камер наблюдения. Здесь же классическая трасология отступает на второй план. Основной массив доказательственной информации сосредоточен в электронной среде: логи транзакций, IP-адреса, хэши блокчейн-операций, история браузера, файлы подкачки операционной системы, дампы оперативной памяти.

Следствие из этого для практики вытекает следующее: следователь, не имеющий специальных познаний в области цифровых технологий, обязан привлекать специалиста уже на этапе осмотра места происшествия (которым может оказаться квартира, где изымается компьютер, или даже отделение банка, откуда проводились операции). Затягивать с этим нельзя — цифровые следы не живут долго. Сессия входа в криптокошелек закрылась, кэш браузера перезаписался, файлы удалены из корзины, и восстановить их становится проблемой даже для эксперта ЭКЦ.

Кроме того, при работе с цифровыми следами действует правило, которое называют «принципом незамедлительности». Если при обычном убийстве следователь может позволить себе осмотреть труп через несколько часов после прибытия на место, то при легализации через криптовалюту промедление в несколько минут может привести к тому, что подозреваемый, узнав о визите оперативников, успеет дистанционно перевести средства на другой адрес. Известны случаи, когда фигуранты удаляли криптокошельки со смартфонов, просто сбрасывая устройство до заводских настроек.

Вторая особенность: трансграничный характер преступной деятельности.

Легализация с использованием криптовалюты почти никогда не ограничивается территорией одного государства, а нередко — и одного региона. Сервер криптобиржи, через которую проходили средства, может находиться на Сейшельских островах или в Сингапуре, оператор электронного кошелька зарегистрирован в Великобритании, а сам преступник, нажимающий на клавиши, сидит где-нибудь в Новосибирске или Барнауле.

Для следователя органов внутренних дел это означает неизбежное столкновение с проблемой получения доказательств из-за рубежа. Направление международного следственного поручения в порядке статьи 453 УПК РФ — процедура долгая и не всегда результативная.

На практике целесообразно, во-первых, использовать открытые источники: блокчейн-обозреватели позволяют проследить движение средств по цепочке адресов даже в случаях, когда биржа находится за рубежом. Во-вторых, необходимо активно взаимодействовать с Национальным центральным бюро Интерпола в России, поскольку такие каналы могут использоваться для получения информации из государств, с которыми прямое взаимодействие затруднено. В-третьих, когда легализация осуществляется через российские обменные пункты, возможно использование предусмотренных законом оперативно-розыскных мероприятий, включая проверочную закупку и оперативный эксперимент.

Третья особенность: высокая степень латентности и сложность выявления момента совершения преступления.

Если кражу или разбой потерпевший обнаруживает практически сразу, то при легализации потерпевшего в классическом понимании этого слова нет. Средства, которые отмываются, изначально были получены преступным путем. Их владелец (тот, кто совершил предикатное преступление) не заявляет в полицию о том, что у него похитили деньги. Наоборот, он всячески скрывает сам факт их существования.

В результате единственными источниками первичной информации о легализации остаются либо сведения от Росфинмониторинга (когда банки фиксируют сомнительные операции), либо результаты оперативно-розыскных мероприятий в рамках расследования предикатного преступления. Это значит, что «автономного» возбуждения уголовного дела по ст. 174 или 174.1 УК РФ, без связи с каким-либо иным преступлением, практически не бывает.

Для следователя данная особенность оборачивается необходимостью доказывать не только сам факт совершения финансовых операций, но и то, что лицо заведомо знало о преступном происхождении средств. При использовании криптовалюты это особенно сложно, поскольку защита часто заявляет: «Мой подзащитный не знал, что биткоины, которые он купил на P2P-бирже, были добыты преступным путем; он просто инвестировал». Разрушить эту версию можно только косвенными доказательствами: завышенной комиссией посредникам, использованием анонимных кошельков, фактом сокрытия следов транзакций через миксеры, перепиской в мессенджерах, где оговаривались условия «безопасного» обмена.

Наиболее наглядно эта проблема проявилась в красноярском деле о майнинге в Богучанском районе. Несмотря на описание обвинением цепочки «незаконно потребленная электроэнергия — биткоин — USDT — наличные и банковские переводы», суд пришел к выводу о недоказанности состава легализации. Следовательно, при расследовании подобных дел необходимо заранее отделять обычное распоряжение преступным доходом или его использование для продолжения преступной деятельности от действий, направленных именно на придание доходу правомерного вида.

Четвертая особенность: необходимость использования специальных познаний в области информационных технологий и финансового мониторинга.

Без привлечения специалиста при расследовании данной категории преступлений обойтись затруднительно. Вместе с тем сохраняется проблема кадрового дефицита специалистов, обладающих одновременно знаниями в

области уголовного процесса, финансового мониторинга, компьютерной техники и блокчейн-аналитики. Поэтому особое значение приобретает подготовка сотрудников оперативных подразделений и экспертно-криминалистических подразделений, способных участвовать в фиксации, изъятии и исследовании цифровых следов.

Пятая особенность: специфика тактики отдельных следственных действий.

Здесь имеет смысл выделить несколько моментов, которые отличают расследование легализации с использованием цифровых инструментов от других экономических преступлений.

Обыск и выемка. При изъятии электронных носителей следователь обязан действовать по заранее согласованному со специалистом алгоритму. Нельзя просто выключить компьютер из розетки — это приведет к потере данных, находящихся в оперативной памяти (а там могут быть как раз пароли и ключи от криптокошельков). Правильный порядок: фото- и видеофиксация рабочего состояния экрана, извлечение дампа оперативной памяти (если есть специалист), затем корректное завершение работы системы, упаковка устройства в антистатический пакет, опечатывание.

Допрос. Особенность допроса по делам о легализации через криптовалюту заключается в необходимости выяснения технических деталей, которые подозреваемый может не помнить или намеренно искажать. Следователю нужно заранее подготовить вопросы о регистрации на биржах (какой адрес электронной почты использовался, какие документы направлялись для верификации), о способах хранения ключей (на бумаге, в файле, в аппаратном кошельке), о комиссиях, которые уплачивались, и о том, почему выбирались именно те или иные сервисы. Ответы на эти вопросы впоследствии сверяются с данными, полученными из оперативных источников.

Назначение экспертизы. Помимо традиционной судебно-экономической экспертизы (которая устанавливает факт проведения финансовых операций и

их несоответствие обычной хозяйственной деятельности), по данной категории дел обязательно назначается компьютерная судебная экспертиза. На разрешение эксперта ставятся вопросы: имеются ли на изъятом носителе программы для работы с криптовалютой, файлы кошельков, история посещения криптобирж и обменников, следы использования миксеров (сервисов по смешиванию транзакций). Эксперт также может дать заключение о том, какие именно операции совершались с конкретного устройства.

После вступления в силу Федерального закона от 20.02.2026 № 38-ФЗ тактика обыска, выемки и осмотра по делам о цифровой валюте должна строиться с учетом ст. 164.2 УПК РФ: изъятие цифровой валюты производится с участием специалиста, материальный носитель хранится в опечатанном виде, а при технической возможности цифровая валюта переводится на специальный адрес-идентификатор. Данное изменение устраняет прежний пробел, но одновременно повышает требования к качеству протокола и квалификации специалиста.

В качестве вывода по параграфу следует отметить, что перечисленные криминалистические особенности не являются разрозненными фактами. Они взаимосвязаны: доминирование цифровых следов порождает необходимость в специальных познаниях, трансграничный характер деятельности осложняет их получение, высокая латентность требует особой тактики следственных действий. Игнорирование хотя бы одной из этих особенностей практически гарантирует, что уголовное дело либо не дойдет до суда, либо вернется на доработку, либо завершится оправдательным приговором.

ЗАКЛЮЧЕНИЕ

Проведенное в рамках настоящей выпускной квалификационной работы исследование, посвященное криминалистической методике расследования легализации денежных средств и иного имущества, совершенной с использованием криптовалюты и электронных платежных средств, позволяет сформулировать ряд выводов теоретического и прикладного характера, а также предложить практические рекомендации, адресованные следственным подразделениям органов внутренних дел.

Актуальность темы, обозначенная во введении, нашла свое подтверждение в ходе анализа следственной и судебной практики. Цифровая трансформация финансовой сферы, с одной стороны, создала удобные инструменты для законопослушных граждан и бизнеса, с другой — была оперативно взята на вооружение криминальными структурами. Традиционные способы отмывания денег, описанные в учебниках криминалистики двадцатилетней давности, постепенно уступают место многоступенчатым схемам с использованием криптовалютных миксеров, электронных кошельков и трансграничных P2P-обменников. Актуальные статистические данные МВД России показывают снижение зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий, однако это не снижает криминалистической значимости проблемы: латентность, трансграничность и сложность доказывания по делам о легализации преступных доходов в цифровой среде сохраняются.

В первой главе работы были рассмотрены теоретико-правовые основы расследования. Уголовно-правовой анализ статей 174 и 174.1 УК РФ показал, что ключевая сложность для правоприменителя заключается в доказывании заведомости — то есть осознания лицом того факта, что имущество или денежные средства получены преступным путем. При использовании цифровой валюты эта сложность сохраняется, однако после изменений 2024–

2026 гг. правовое регулирование стало более определенным: закреплены нормы о майнинге и майнинг-пулах, обязанность представления сведений о полученной цифровой валюте и адресах-идентификаторах, возможность специальных расчетов цифровой валютой в рамках экспериментальных правовых режимов, а также признание цифровой валюты имуществом для целей УК РФ и УПК РФ. Разработанная в параграфе 1.3 криминалистическая классификация преступлений данного вида создает основу для дифференцированного подхода к расследованию в зависимости от используемого инструментария (исключительно цифровая валюта, исключительно электронные платежные средства либо смешанные схемы).

Вторая глава была посвящена непосредственно элементам частной криминалистической методики. Криминалистическая характеристика, представленная в параграфе 2.1, позволила систематизировать сведения о способах совершения (конверсия через криптовалюту, структурирование через электронные платежные средства, смешанные многоступенчатые схемы), обстановке (виртуальная трансграничная среда), предмете (цифровые активы и электронные денежные средства), личности преступника (профессиональные участники с ИТ-образованием и «дропы» — номинальные держатели) и механизме цифрового слеодообразования. Особо подчеркнем, что именно последний элемент — цифровые следы в блокчейне, у операторов связи и на устройствах пользователей — является тем «слабым звеном» преступников, грамотная работа с которым может обеспечить успех всего расследования.

Анализ типичных следственных ситуаций (параграф 2.2) показал, что следователь сталкивается с принципиально разными условиями работы в зависимости от источника первичной информации. Если дело «пришло» из Росфинмониторинга — одна тактика, если легализация выявлена в рамках расследования предикатного преступления — иная, а если поступила оперативная информация о деятельности организованной группы «отмывателей» — третья. Универсального рецепта нет и быть не может.

Однако выделение этих ситуаций позволяет следователю не действовать вслепую, а изначально выбирать те следственные действия и оперативно-розыскные мероприятия, которые в данной ситуации дают максимальный результат.

Система тактических задач, рассмотренная в параграфе 2.3, структурирует деятельность следователя на информационно-поисковом, обеспечительном, удостоверительном и организационно-управленческом уровнях. Наиболее важным для практической работы является выделение обеспечительных задач — задач по сохранению цифровых доказательств, изъятию носителей информации, фиксации адресов-идентификаторов и наложению ареста на цифровую валюту. С учетом изменений 2026 года следователь должен применять специальные правила изъятия цифровой валюты с участием специалиста, обеспечивать сохранность данных доступа и своевременно обращаться в суд с ходатайством о наложении ареста, поскольку промедление позволяет фигуранту перевести активы на неконтролируемый адрес.

Криминалистические особенности расследования, описанные в параграфе 2.4 (доминирование цифровых следов, трансграничный характер, высокая латентность, необходимость специальных познаний и специфика тактики следственных действий), представляют собой те «болевые точки», которые требуют первоочередного внимания как со стороны законодателя, так и со стороны руководства следственных подразделений. Без решения проблемы подготовки кадров, способных работать с блокчейн-транзакциями, и без оснащения экспертно-криминалистических подразделений современным программным обеспечением эффективность расследования данной категории преступлений будет оставаться ограниченной.

Практические рекомендации, которые вытекают из проведенного исследования и могут быть предложены для внедрения в деятельность следственных подразделений органов внутренних дел, сводятся к следующему.

На этапе доследственной проверки при поступлении информации от Росфинмониторинга или из иных источников незамедлительно направлять запросы в кредитные организации и операторов электронных платежных систем с требованием предоставить расширенные выписки по счетам всех фигурантов, включая IP-адреса, с которых осуществлялся доступ.

При возбуждении уголовного дела по ст. 174 или 174.1 УК РФ одновременно давать поручение органу дознания о проведении оперативно-розыскных мероприятий, направленных на установление всех звеньев транзакционной цепочки, включая возможные факты использования криптовалютных миксеров и зарубежных бирж.

В ходе обыска у подозреваемых обязательно привлекать специалиста в области информационных технологий. Изъятие электронных устройств производить с соблюдением правил, исключающих утрату данных, находящихся в оперативной памяти. Все изъятые носители упаковывать и опечатывать с составлением отдельного протокола.

При обнаружении цифровой валюты на аппаратных или программных кошельках незамедлительно обеспечивать участие специалиста, фиксировать адрес-идентификатор, закрытые данные доступа, устройство и последовательность действий при обнаружении цифровой валюты. После этого в порядке ст. 115 УПК РФ необходимо обращаться в суд с ходатайством о наложении ареста на цифровую валюту, обосновывая, что она является предметом преступного посягательства, получена в результате преступления либо используется для легализации преступных доходов. При наличии технической возможности следует ставить вопрос о переводе цифровой валюты на адрес-идентификатор для обеспечения ее сохранности.

Допрос подозреваемого (обвиняемого) строить по принципу последовательной детализации, задавая вопросы о каждом звене финансовой операции: с какого устройства, через какую биржу или обменник, с какого адреса кошелька, с уплатой какой комиссии, в какое время суток и с какого IP-адреса производились действия. Расхождения между показаниями и

объективными данными (логами, выписками, данными блокчейн-обозревателей) фиксировать и использовать для изобличения.

В обязательном порядке назначать комплексную судебную экспертизу, включающую компьютерно-техническое исследование изъятых устройств и экономическое исследование финансовых операций. Вопросы экспертам формулировать совместно со специалистом, чтобы избежать двусмысленности.

При анализе операций с цифровой валютой использовать возможности блокчейн-аналитики и информационного взаимодействия с Росфинмониторингом. Полученные с помощью аналитических инструментов сведения должны использоваться как ориентирующая и проверочная информация, а для придания им доказательственного значения необходимо закреплять их процессуальными средствами: протоколами осмотра, заключениями экспертов, ответами на запросы и иными предусмотренными УПК РФ доказательствами.

В случаях, когда транзакции выходят за пределы юрисдикции РФ, направлять международные следственные поручения в порядке ст. 453 УПК РФ, одновременно используя возможности Национального центрального бюро Интерпола и не пренебрегая открытыми блокчейн-обозревателями, которые часто дают информацию, достаточную для формирования внутреннего убеждения следователя и суда.

Анализ судебной практики 2025–2026 гг. показывает, что для успешной квалификации по ст. 174 или 174.1 УК РФ недостаточно установить сам факт движения цифровой валюты, ее конвертации или последующего получения рублей. Ключевым является доказывание специальной цели легализации: сокрытия преступного происхождения имущества, маскировки маршрута его движения и создания видимости законности владения, пользования и распоряжения им.

Завершая работу, хотелось бы подчеркнуть, что расследование легализации денежных средств и иного имущества с использованием

криптовалюты и электронных платежных средств — это та область, где теоретические знания напрямую переходят в практический результат. Преступники, осваивающие новые технологии, не стоят на месте. Следовательно, не может стоять на месте и методика их разоблачения. Именно динамичность, готовность к постоянному обучению и тесное взаимодействие с оперативными подразделениями и экспертными учреждениями составляют залог успеха в противодействии этому опасному виду экономической преступности. Поставленные в исследовании задачи выполнены, цель достигнута, а сформулированные выводы и рекомендации могут быть использованы как в практической деятельности следственных подразделений, так и в учебном процессе при подготовке будущих офицеров органов внутренних дел.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации : принята всенародным голосованием 12.12.1993 // СПС КонсультантПлюс.
2. Уголовный кодекс Российской Федерации : Федеральный закон от 13.06.1996 № 63-ФЗ // СПС КонсультантПлюс.
3. Уголовно-процессуальный кодекс Российской Федерации : Федеральный закон от 18.12.2001 № 174-ФЗ // СПС КонсультантПлюс.
4. О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма : Федеральный закон от 07.08.2001 № 115-ФЗ // СПС КонсультантПлюс.
5. О национальной платежной системе : Федеральный закон от 27.06.2011 № 161-ФЗ // СПС КонсультантПлюс.
6. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 31.07.2020 № 259-ФЗ // СПС КонсультантПлюс.
7. Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации : Федеральный закон от 31.07.2020 № 258-ФЗ // СПС КонсультантПлюс.
8. О внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 08.08.2024 № 221-ФЗ // СПС КонсультантПлюс.
9. О внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 08.08.2024 № 223-ФЗ // СПС КонсультантПлюс.

10. О внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 25.10.2024 № 349-ФЗ // СПС КонсультантПлюс.

11. О внесении изменений в части первую и вторую Налогового кодекса Российской Федерации и отдельные законодательные акты Российской Федерации : Федеральный закон от 29.11.2024 № 418-ФЗ // СПС КонсультантПлюс.

12. О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации : Федеральный закон от 20.02.2026 № 38-ФЗ // СПС КонсультантПлюс.

13. О внесении изменения в статью 29 Гражданского процессуального кодекса Российской Федерации : Федеральный закон от 04.07.2026 № 223-ФЗ // СПС КонсультантПлюс.

14. О Стратегии экономической безопасности Российской Федерации на период до 2030 года : Указ Президента Российской Федерации от 13.05.2017 № 208 // СПС КонсультантПлюс.

15. О Стратегии национальной безопасности Российской Федерации : Указ Президента Российской Федерации от 02.07.2021 № 400 // СПС КонсультантПлюс.

16. Концепция развития национальной системы противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма : утверждена Президентом Российской Федерации 30.05.2018 // СПС КонсультантПлюс.

17. О внесении изменения в постановление Правительства Российской Федерации от 23 декабря 2024 г. № 1869 : постановление Правительства Российской Федерации от 18.03.2026 № 280 // СПС КонсультантПлюс.

18. О внесении изменений в некоторые постановления Пленума Верховного Суда Российской Федерации по уголовным делам : постановление Пленума Верховного Суда Российской Федерации от 16.06.2026 № 30 // СПС КонсультантПлюс.

19. О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем : постановление Пленума Верховного Суда Российской Федерации от 07.07.2015 № 32 // СПС КонсультантПлюс.

20. Информационное письмо от 19.06.2026 № 69 «Методические рекомендации по применению субъектами исполнения Федерального закона от 07.08.2001 № 115-ФЗ мер по замораживанию (блокированию) денежных средств или иного имущества и снятию таких мер, а также приостановлению операций с денежными средствами или иным имуществом» // СПС КонсультантПлюс.

Монографии, учебники, учебные пособия

21. Белкин, Р.С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики : монография / Р.С. Белкин. – М. : Норма-Инфра, 2001. – 240 с.

22. Земцова, С.И. Криптовалюта как объект криминалистического исследования при расследовании преступлений в сфере незаконного оборота наркотических средств и психотропных веществ : учебное пособие / С.И. Земцова, П.В. Галушин, А.Л. Карлов. – Красноярск : СибЮИ МВД России, 2021. – 104 с.

23. Корноухов, В.Е. Курс криминалистики. Особенная часть. Т. 2. Методики расследований преступлений в сфере экономики, охраны труда, пожарной безопасности, экологии и транспорта / отв. ред. В.Е. Корноухов. – М. : Юристъ, 2004. – 541 с.

24. Криминалистика : учебник для вузов / под ред. А.Г. Филиппова. – 3-е изд., перераб. и доп. – М. : Издательство Юрайт, 2025. – 402 с.

25. Лопашенко, Н.А. Преступления в сфере экономической деятельности: теоретический и прикладной анализ : монография / Н.А. Лопашенко. – Ч. 1. – М. : Юрлитинформ, 2015. – 330 с.

26. Фойницкий, И.Я. Курс уголовного права. Часть Особенная. Посягательства личные и имущественные : учебник / И.Я. Фойницкий. – Петроград : Юрид. о-во при Петрогр. ун-ве, 1916. – 439 с.

Научные публикации и статьи в иных периодических изданиях

27. Архипов, А.В. Ответственность за хищение безналичных и электронных денежных средств: новеллы законодательства / А.В. Архипов // Уголовное право. – 2018. – № 3. – С. 4–9.

28. Бисултанова, А.А. Криптовалюты: история, предпосылки / А.А. Бисултанова // Экономика и бизнес: теория и практика. – 2024. – № 6-1 (112). – С. 75–77.

29. Васильева, О.Н. Особенности установления и доказывания легализации (отмывания) денежных средств с использованием криптовалют / О.Н. Васильева, М.М. Милованова // Евразийская адвокатура. – 2023. – № 6 (65). – С. 68–71.

30. Вильская, Н.В. О некоторых особенностях криминалистической характеристики преступлений, совершенных с использованием криптовалют / Н.В. Вильская, В.Ю. Малахова // Проблемы экономики и юридической практики. – 2024. – № 1. – С. 94–101.

31. Жамбалов, Д.Б. Криминалистическая характеристика легализации (отмывания) доходов, полученных преступным путем / Д.Б. Жамбалов // Вестник Восточно-Сибирского института МВД России. – 2019. – № 4 (91). – С. 159–168.

32. Кесарева, Г.Ю. Криминалистическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет : дис. ... канд. юрид. наук / Г.Ю. Кесарева. – М., 2002. – С. 101–105.

33. Макаров, А.В. Особенности и проблемы квалификации мошенничества, совершенного с использованием электронных средств платежа / А.В. Макаров, В.А. Алешкова // Российский судья. – 2019. – № 5. – С. 24–29.

34. Миллос, А.И. Современные способы легализации денежных средств, полученных преступным путем / А.И. Миллос // Актуальные проблемы борьбы с преступностью: вопросы теории и практики : материалы XXVIII Международной научно-практической конференции : в 2 ч. – Красноярск, 2025. – С. 270–272.

35. Некрасов, Д.Е. Электронные денежные средства как предмет преступления / Д.Е. Некрасов, А.А. Брюханов, И.П. Напханенко // ЮП. – 2023. – № 4 (107). – С. 167–174.

36. Шашкова, А.В. Зарождение понятия «легализация (отмывание) доходов, полученных преступным путем» / А.В. Шашкова // Вестник МГИМО. – 2011. – № 3. – С. 272–274.

Интернет-ресурсы

37. Информационное сообщение Росфинмониторинга от 16.05.2025 «О необходимости подключения лиц, осуществляющих майнинг цифровой валюты (в том числе участников майнинг-пула) и лиц, организующих деятельность майнинг-пула, при распределении ими выпущенной (полученной) цифровой валюты между участниками майнинг-пула к личному кабинету на официальном сайте Федеральной службы по финансовому мониторингу» // Росфинмониторинг : [Электронный ресурс]. – URL: <https://www.fedsfm.ru/news/8769> (дата обращения: 18.06.2026).

38. МВД России публикует статистическую информацию о состоянии преступности в Российской Федерации за январь–май 2026 года // МВД МЕДИА : [Электронный ресурс]. – 17.06.2026. – URL:

<https://mvdmedia.ru/news/official/mvd-rossii-publikuet-statisticheskuyu-informatsiyu-o-sostoyanii-prestupnosti-/> (дата обращения: 18.06.2026).

39. Программа для ЭВМ «Прозрачный блокчейн. Государственный модуль» // Росфинмониторинг : [Электронный ресурс]. – URL: <https://www.fedsfm.ru/activity/informational-systems/pb-gos-modul> (дата обращения: 18.06.2026).

40. Состояние преступности (архивные данные) Министерства внутренних дел Российской Федерации // МВД России : [Электронный ресурс]. – URL: <https://мвд.рф/folder/101762> (дата обращения: 18.06.2026).

41. Статистические сведения о состоянии преступности в 2025 году // МВД МЕДИА : [Электронный ресурс]. – 29.01.2026. – URL: <https://mvdmedia.ru/news/official/statisticheskie-svedeniya-o-sostoyanii-prestupnosti-v-2025-godu/> (дата обращения: 18.06.2026).

Эмпирические материалы

42. Апелляционное постановление Ярославского областного суда от 20.04.2025 по делу № 1-51/2025 // СудАкт : [Электронный ресурс]. – URL: <https://sudact.ru/regular/doc/wkmsreIoJFQ3/> (дата обращения: 18.06.2026).

43. Приговор Богучанского районного суда Красноярского края от 27.01.2026 по делу № 1-12/2026 (12402040020000034).

44. Приговор Городищенского районного суда Волгоградской области от 02.06.2025 по делу № 1-140/2025 // СудАкт : [Электронный ресурс]. – URL: <https://sudact.ru/regular/doc/NgxoeUAjH7b8/> (дата обращения: 18.06.2026).

45. Приговор Останкинского районного суда г. Москвы от 11.08.2025 по делу № 01-0570/2025 // СудАкт : [Электронный ресурс]. – URL: <https://sudact.ru/regular/doc/jd9OqWoMBA1r/> (дата обращения: 18.06.2026).

46. Приговор Центрального районного суда г. Читы Забайкальского края от 29.08.2025 по делу № 1-125/2025 // СудАкт : [Электронный ресурс]. – URL: <https://sudact.ru/regular/doc/RUuodGTO0411/> (дата обращения: 18.06.2026).